ENCYCLOPEDIA OF
Espionage, Intelligence, and Security

ENCYCLOPEDIA OF
Espionage, Intelligence, and Security

This page intentionally left blank

ENCYCLOPEDIA OF
Espionage, Intelligence, and Security

K. LEE LERNER AND BRENDA WILMOTH LERNER, EDITORS

volume
III
R–Z
INDEX

Detroit • New York • San Diego • San Francisco • Cleveland • New Haven, Conn. • Waterville, Maine • London • Munich

Encyclopedia of Espionage, Intelligence, and Security

K. Lee Lerner and Brenda Wilmoth Lerner, editors

Project Editor
Stephen Cusack

Editorial
Erin Bealmear, Joann Cerrito, Jim Craddock, Miranda Ferrara, Kristin Hart, Melissa Hill, Carol Schwartz, Christine Tomassini, Michael J. Tyrkus, Peter Gareffa

Permissions
Lori Hines

Imaging and Multimedia
Dean Dauphinais, Leitha Etheridge-Sims, Mary K. Grimes, Lezlie Light, Luke Rademacher

Product Design
Kate Scheible

Manufacturing
Rhonda Williams

For more information, contact
The Gale Group, Inc.
27500 Drake Rd.
Farmington Hills, MI 48331-3535
Or you can visit our Internet site at http://www.gale.com

Cover Photos

Volume 1: Ethel and Julius Rosenberg following arraignment on charges of espionage, August 23, 1950. ©Bettmann/Corbis

Volume 2: SR-71 Blackbird, c. 1991. ©Corbis

Volume 3: Clean-up crews scour the American Media Inc. building in Boca Raton, Florida, after the discovery of anthrax spores, October 9, 2001. AP/Wide World Photos.

Library of Congress Cataloging-in-Publication Data

Encyclopedia of espionage, intelligence, and security / K. Lee Lerner and Brenda Wilmoth Lerner, editors.
p. cm.
Includes bibliographical references and index.
ISBN 0-7876-7546-6 (set : hardcover : alk. paper) — ISBN 0-7876-7686-1 (v. 1) — ISBN 0-7876-7687-X (v. 2) — ISBN 0-7876-7688-8 (v. 3)
1. Espionage—Encyclopedias. 2. Intelligence service—Encyclopedias. 3. Security systems—Encyclopedias. I. Lerner, K. Lee. II. Lerner, Brenda Wilmoth.
JF1525.I6E63 2004
327.12'03—dc21

2003011097

This title is available as an e-book.
ISBN 0-7876-7762-0

Contact your Gale sales representative for ordering information.

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

Contents

INTRODUCTION VII

ADVISORS AND CONTRIBUTORS XI

LIST OF ENTRIES XIII

The Encyclopedia of Espionage, Intelligence, and Security 1

GLOSSARY 289

CHRONOLOGY 317

SOURCES 353

INDEX 403

This page intentionally left blank

Introduction

In composing *The Encyclopedia of Espionage, Intelligence, and Security (EEIS),* our goal was to shape a modern encyclopedia offering immediate value to our intended readers by emphasizing matters of espionage, intelligence, and security most frequently in the news.

EEIS is not intended as a classical "spy book," filled with tales of daring operations. Instead, within a framework of historical overviews, *EEIS* emphasizes the scientific foundations, applications of technology, and organizational structure of modern espionage, intelligence, and security. High school and early undergraduate students can use this book to expand upon their developing awareness of the fundamentals of science, mathematics, and government as they begin the serious study of contemporary issues.

EEIS is also intended to serve more advanced readers as a valuable quick reference and as a foundation for advanced study of current events.

EEIS devotes an extensive number of articles to agencies and strategies involved in emerging concepts of homeland security in the United States. Faced with a daunting amount of information provided by agencies, organizations, and institutes seeking to put their best foot forward, we have attempted to allocate space to the topics comprising *EEIS* based upon their relevance to some unique facet of espionage, intelligence, or security—especially with regard to science and technology issues—as opposed to awarding space related to power of the agency or availability of material.

A fundamental understanding of science allows citizens to discern hype and disregard hysteria, especially with regard to privacy issues. Spy satellites powerful enough to read the details of license plates do so at peril of missing events a few steps away. With regard to electronic intercepts, the capability to identify what to carefully examine—often a decision driven by mathematical analysis—has become as essential as the capacity to gather the intelligence itself. Somewhere between the scrutiny of Big Brother and the deliberately blind eye lie the shadows into which terrorists often slip.

With an emphasis on the realistic possibilities and limitations of science, we hope that *EEIS* finds a useful and unique place on the reference shelf.

It seems inevitable that within the first half of the twenty-first century, biological weapons may eclipse nuclear and chemical weapons in terms of potential threats to civilization. Because informed and reasoned public policy debates on issues of biological warfare and bioterrorism can only take place when there is a fundamental understanding of the science underpinning competing arguments, *EEIS* places special emphasis on the multifaceted influence and applications of the biological sciences and emerging biometric technologies. Future generations of effective intelligence and law enforcement officers seeking to thwart the threats posed by tyrants, terrorists, and the technologies of mass destruction might be required to be as knowledgeable in the terminology of epidemiology as they are with the tradecraft of espionage.

Knowledge is power. In a time where news can overwhelm and in fact, too easily mingle with opinion, it is our hope that *EEIS* will provide readers with greater insight to measure vulnerability and risks, and correspondingly, an increased ability to make informed judgments concerning the potential benefits and costs of espionage, intelligence, and security matters.

K. LEE LERNER & BRENDA WILMOTH LERNER, EDITORS
CORNWALL, U.K.
MAY, 2003

How to Use the Book

The *Encyclopedia of Espionage, Intelligence, and Security* was not intended to contain a compendium of weapons systems. Although *EEIS* carries brief overviews of specifically selected systems commonly used in modern intelligence operations, readers interested in detailed information regarding weapons systems are recommended

to *Jane's Strategic Weapon Systems*, or *Jane's Defense Equipment Library*.

Although *EEIS* contains overview of significant historical periods and events, for those readers interested in additional information regarding the history of espionage operations and biographies of intelligence personnel, the editors recommend Jeffrey T. Richelson's *A Century of Spies : Intelligence in the Twentieth Century* (Oxford University Press, 1995), Vincent Buranelli and Nan Buranelli's *Spy/Counterspy: An Encyclopedia of Espionage* (New York: McGraw-Hill, 1982), and Allen Dulles', *The Craft of Intelligence* (New York: Harper & Row, 1963).

The articles in *EEIS* are meant to be understandable by anyone with a curiosity about topics in espionage, intelligence, and security matters, and this first edition of the book has been designed with ready reference in mind:

- Entries are arranged alphabetically. In an effort to facilitate easy use of this encyclopedia, and to attempt order in a chaotic universe of names and acronyms the editors have adopted a "common use" approach. Where an agency, organization, or program is known best by its acronym, the entry related to that organization will be listed by the acronym (e.g. FEMA is used instead of Federal Emergency Management Agency). To facilitate use, the editors have included a number of "jumps" or cross-referenced titles that will guide readers to desired entries.
- To avoid a log jam of terms starting with "Federal" and "United States," titles were broken to most accurately reflect the content emphasized or subject of agency authority.
- **"See Also" references** at the end of entries alert the readers to related entries not specifically mentioned in the body of the text that may provide additional or interesting resource material.
- An extensive **Glossary** of terms and acronyms is included to help the reader navigate the technical information found in *EEIS*.
- The **Chronology** includes significant events related to the content of the encyclopedia. Often accompanied by brief explanations, the most current entries date represent events that occurred just as *EEIS* went to press.
- A **Sources** section lists the most worthwhile print material and web sites we encountered in the compilation of this volume. It is there for the inspired reader who wants more information on the people and discoveries covered in this volume.
- A comprehensive general **Index** guides the reader to topics and persons mentioned in the book. Bolded page references refer the reader to the term's full entry.
- The editors and authors have attempted to explain scientific concepts clearly and simply, without sacrificing fundamental accuracy. Accordingly, an advanced understanding of physics, chemistry, or biochemistry is not assumed or required. Students and other readers should not, for example, be intimidated or deterred by the complex names of biochemical molecules—where necessary for complete understanding, sufficient information regarding scientific terms is provided.
- To the greatest extent possible we have attempted to use Arabic names instead of their Latinized versions. Where required for clarity we have included Latinized names in parentheses after the Arabic version. Alas, we could not retain some diacritical marks (e.g. bars over vowels, dots under consonants). Because there is no generally accepted rule or consensus regarding the format of translated Arabic names, we have adopted the straightforward, and we hope sensitive, policy of using names as they are used or cited in their region of origin.
- EEIS relies on open source material and no classified or potentially dangerous information is included. Articles have been specifically edited to remove potential "how to" information. All articles have been prepared and reviewed by experts who were tasked with ensuring accuracy, appropriateness, and accessibility of language.
- With regard to entries regarding terrorist organizations, *EEIS* faced a serious dilemma. For obvious reasons, it was difficult to obtain balanced, impartial, and independently verifiable information regarding these organizations, nor could *EEIS* swell to incorporate lengthy scholarly analysis and counter-analysis of these organizations without losing focus on science and technology issues. As a compromise intended to serve students and readers seeking initial reference materials related to organizations often in the news, *EEIS* incorporates a series of supplemental articles to convey the information contained in the U.S. Department of State annual report to Congress titled, *Patterns of Global Terrorism,* 2001. These articles contain the language, assertions of fact, and views of the U.S. Department of State. Readers are encouraged to seek additional information from current U.S. Department of State resources and independent non-governmental scholarly publications that deal with the myriad of issues surrounding the nature and activities of alleged terrorist organizations. A number of governmental and non-governmental publications that deal with these issues are cited in the bibliographic sources section located near the index.

Key *EEIS* articles are signed by their authors. Brief entries were compiled by experienced researchers and reviewed by experts. In the spirit of numerous independent scientific watchdog groups, during the preparation of *EEIS* no contributors held a declared affiliation with any intelligence or security organization. This editorial policy not only allowed a positive vetting of contributors, but also assured an independence of perspective and an emphasis on the fundamentals of science as opposed to unconfirmable "insider" information.

When the only verifiable or attributable source of information for an entry comes from documents or information provided by a governmental organization (e.g., the U.S. Department of State), the editors endeavored to carefully note when the language used and perspective offered was that of the governmental organization.

Although some research contributors requested anonymity, no pseudonyms are used herein.

Acknowledgments

The editors wish to thank Herbert Romerstein, former USIA Soviet Disinformation Officer and Coordinator of Programs to Counter Soviet Active Measures, United States Information Agency, for his assistance in compiling selected articles.

The editors wish to thank Lee Wilmoth Lerner for his assistance in compiling technical engineering data for inclusion in EEIS.

The editors acknowledge the assistance of the members of the Federation of American Scientists for the provision of reports and materials used in the preparation of selected articles.

Although certainly not on the scale of the challenge to provide security for a nation with approximately 85 deep-draft ports, 600,000 bridges, 55,000 independent water treatment systems, 100 nuclear power plants, and countless miles of tunnels, pipelines, and electrical and communications infrastructure, the task of incorporating changes brought on by creation of the Department of Homeland Security—and the most massive reorganization of the United States government since World War II—as this book went to press provided a unique challenge to *EEIS* writers and advisors. The editors appreciate their dedication and willingness to scrap copy, roll up their sleeves, and tackle anew the smorgasbord of name and terminology changes.

As publishing deadlines loomed, EEIS was also well served by a research staff dedicated to incorporating the latest relevant events—especially information related to the search for weapons of mass destruction—that took place during war in Iraq in March and April of 2003.

EEIS advisors, researchers, and writers tenaciously attempted to incorporate the most current information available as *EEIS* went to press. The editors pass any credit or marks for success in that effort, and reserve for themselves full responsibility for omissions.

The editors gratefully acknowledge the assistance of many at St. James Press for their help in preparing *The Encyclopedia of Espionage, Intelligence, and Security*. The editors extend thanks to Mr. Peter Gareffa and Ms. Meggin Condino for their faith in this project. Most directly, the editors wish to acknowledge and thank the project editor, Mr. Stephen Cusack, for his talented oversight and for his tireless quest for secure engaging pictures for *EEIS*.

The editors lovingly dedicate this book to the memory of Wallace Schaffer, Jr., HM3, USNR, who died on January 8, 1968, in Thua Thien (Hue) Province, Vietnam.

"A small rock holds back a great wave."—Homer, *The Odyssey*.

This page intentionally left blank

Advisors and Contributors

Julie Berwald, Ph.D.
Geophysicist, writer on marine science, environmental biology, and issues in geophysics.
Austin, Texas

Robert G. Best, Ph.D.
Clinical cytogeneticist and medical geneticist who has written on a range of bioscience issues
Director, Division of Genetics
University of South Carolina School of Medicine

Tim Borden, Ph.D.
Doctorate in History from Indiana University, and is an inspector with the U.S. Bureau of Customs and Border Protection
Toledo, Ohio

Brian Cobb, Ph.D.
Bioscience writer, researcher
Institute for Molecular and Human Genetics
Georgetown University, Washington, D.C.

Cecilia Colomé, Ph.D.
Astrophysicist, translator, and science writer
Austin, Texas

Laurie Duncan, Ph.D.
Geologist, science writer, and researcher
Austin, Texas

William J. Engle, P.E.
Writer on contemporary geophysics issues and the impacts of science and technology on history
Exxon-Mobil Oil Corporation (Rt.) New Orleans, Louisiana

Antonio Farina, M.D., Ph.D.
Physician, researcher, and writer on medical science issues
Assistant Professor, University of Bologna, Italy

Christopher T. Fisher, Ph.D.
Assistant Professor, Department of African American Studies and the Department of History
The College of New Jersey, Ewing, New Jersey

Larry Gilman, Ph.D.
Electrical engineer and science writer
Sharon, Vermont

William Haneberg, Ph.D.
Former research scientist and professor, now an independent consulting geologist and science writer
Portland, Oregon

Brian D. Hoyle, Ph.D.
Science writer and Chief Microbiologist, Government of New Brunswick from 1993 to 1997
Nova Scotia, Canada

Joseph Patterson Hyder
Writer on the historical impacts of science and technology
University of Tennessee College of Law, Knoxville, Tennessee

Alexandr Ioffe, Ph.D.
Writer on the history of science and researcher with the Geological Institute of Russian Academy of Sciences in Moscow
Russian Academy of Sciences, Moscow

Judson Knight
Science writer, researcher, and editor
Knight Agency Research Services, Atlanta, Georgia

Michael Lambert, Ph.D.
Researcher at the Great Plains/Rocky Mountain Hazardous Substance Research Center and at the U.S. Naval Research Laboratory
Manhattan, Kansas

Adrienne Wilmoth Lerner
Writer of various articles on the history of science, archaeology, and the evolution of security-related law
University of Tennessee College of Law, Knoxville, Tennessee

Agnes Lichanska, Ph.D.
Science writer who has conducted research at the Department of Medical Genetics and Ophthalmology at Queen's University of Belfast (Northern Ireland)
University of Queensland, Brisbane, Australia

Eric v.d. Luft, Ph.D., M.L.S.
Writer on cultural, scientific, and intellectual history, and philosophy
Curator of Historical Collections
SUNY Upstate Medical University, Syracuse, New York

Martin Manning
Served on the Economic Security Team, Office of International Information Programs, U.S. Department of State
Bureau of Public Diplomacy
U.S. Department of State, Washington, D.C.

Kelli Miller
Served as news writer and producer for Inside Science *TV News at the American Institute of Physics (AIP) and as executive producer of* Discoveries & Breakthroughs Inside Science
Atlanta, Georgia

Caryn E. Neumann
Instructor and doctoral candidate in the Department of History at Ohio State University
Columbus, Ohio

Mike O'Neal, Ph.D.
Independent scholar and writer
Moscow, Idaho

Belinda M. Rowland, Ph.D.
Science and medical writer
Voorheesville, New York

Judyth Sassoon, Ph.D., ARCS
Science writer with research experience in NMR and X-ray crystallography techniques
Department of Biology & Biochemistry
University of Bath, United Kingdom

Morgan Simpson
Aerospace Engineer
National Aeronautical and Space Administration (NASA)
Kennedy Space Center, Cape Canaveral, Florida

Constance K. Stein, Ph.D.
Writer on medical and bioscience issues related to modern genetics
Director of Cytogenetics, Assistant Director of Molecular Diagnostics
SUNY Upstate Medical University, Syracuse, New York

Tabitha Sparks, Ph.D.
Marion L. Brittain fellow, Georgia Institute of Technology and Fellow, Center for Humanistic Inquiry, Emory University
Atlanta, Georgia

David Tulloch
Science and technology writer
Wellington, New Zealand

Michael T. Van Dyke, Ph.D.
Served as visiting assistant professor, Department of American Thought & Language
Michigan State University, East Lansing, Michigan

Stephanie Watson
Science writer specializing in the social impacts of science and technology
Smyrna, Georgia

Simon Wendt, Ph.D.
Ph.D. candidate in Modern History and History instructor
John F. Kennedy Institute for North American Studies, Free University of Berlin, Germany

List of Entries

A

Abu Nidal Organization (ANO)
Abu Sayyaf Group (ASG)
Abwehr
ADFGX Cipher
Aflatoxin
Africa, Modern U.S. Security Policy and Interventions
Agent Orange
Air and Water Purification, Security Issues
Air Force Intelligence, United States
Air Force Office of Special Investigations, United States
Air Marshals, United States
Air Plume and Chemical Analysis
Aircraft Carrier
Airline Security
Al-Aqsa Martyrs Brigade
Alex Boncayao Brigade (ABB)
Al-Gama'a al-Islamiyya (Islamic Group, IG)
Al-Ittihad al-Islami (AIAI)
Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya
Al-Jihad
Allied Democratic Forces (ADF)
Al-Qaeda (also known as Al-Qaida)
Americas, Modern U.S. Security Policy and Interventions
Ames (Aldrich H.) Espionage Case
Anthrax
Anthrax, Terrorist Use as a Biological Weapon
Anthrax Vaccine
Anthrax Weaponization
Antiballistic Missile Treaty
Antibiotics
Anti-Imperialist Territorial Nuclei (NTA)
APIS (Advance Passenger Information System)
Archeology and Artifacts, Protection of during War
Architecture and Structural Security
Area 51 (Groom Lake, Nevada)
Argentina, Intelligence and Security
Argonne National Laboratory
Armed Islamic Group (GIA)
Arms Control, United States Bureau
Army for the Liberation of Rwanda (ALIR)
Army Security Agency
'Asbat al-Ansar
Asilomar Conference
Assassination
Assassination Weapons, Mechanical
Asymmetric Warfare
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)
Atmospheric Release Advisory Capability (ARAC)
Audio Amplifiers
Aum Supreme Truth (Aum)
Australia, Intelligence and Security
Austria, Intelligence and Security
Aviation Intelligence, History
Aviation Security Screeners, United States

B

B-2 Bomber
B-52
Bacterial Biology
Ballistic Fingerprints
Ballistic Missile Defense Organization, United States
Ballistic Missiles
Balloon Reconnaissance, History
Basque Fatherland and Liberty (ETA)
Bathymetric Maps
Bay of Pigs
Belgium, Intelligence and Security Agencies
Belly Buster Hand Drill
Berlin Airlift
Berlin Tunnel
Berlin Wall
Biochemical Assassination Weapons
Biocontainment Laboratories
Biodetectors
Bio-Engineered Tissue Constructs
Bio-Flips
Biological and Biomimetic Systems
Biological and Toxin Weapons Convention
Biological Input/Output Systems (BIOS)

Biological Warfare
Biological Warfare, Advanced Diagnostics
Biological Weapons, Genetic Identification
Bio-Magnetics
Biomedical Technologies
Biometrics
Bio-Optic Synthetic Systems (BOSS)
Biosensor Technologies
BioShield Project
Bioterrorism
Bioterrorism, Protective Measures
Black Chamber
Black Ops
Black Tom Explosion
Bletchley Park
Bolivia, Intelligence and Security
Bomb Damage, Forensic Assessment
Bomb Detection Devices
Bombe
Bosnia and Herzegovina, Intelligence and Security
Botulinum Toxin
Brain-Machine Interfaces
Brain Wave Scanners
Brazil, Intelligence and Security
British Terrorism Act
Brookhaven National Laboratory
Bubonic Plague
Bugs (Microphones) and Bug Detectors
Bush Administration (1989–1993), United States National Security Policy
Bush Administration (2001–), United States National Security Policy

C

Cambodian Freedom Fighters (CFF)
Cambridge University Spy Ring
Cameras
Cameras, Miniature
Canada, Counter-Terrorism Policy
Canada, Intelligence and Security
Canine Substance Detection
Carter Adminstration (1977–1981), United States National Security Policy
CDC (United States Centers for Disease Control and Prevention)
CERN
Chechen-Russian Conflict
Chemical and Biological Defense Information Analysis Center (CBIAC)
Chemical and Biological Detection Technologies
Chemical Biological Incident Response Force, United States
Chemical Safety and Hazard Investigation Board (USCSB), United States
Chemical Safety: Emergency Responses
Chemical Warfare
Chemistry: Applications in Espionage, Intelligence, and Security Issues
Chernobyl Nuclear Power Plant Accident, Detection and Monitoring
Chile, Intelligence and Security
China, Intelligence and Security
Chinese Espionage against the United States
Church Committee
CIA (United States Central Intelligence Agency)
CIA (CSI), Center for the Study of Intelligence
CIA Directorate of Science and Technology (DS&T)
CIA, Foreign Broadcast Information Service
CIA, Formation and History
CIA, Legal Restriction
Cipher Disk
Cipher Key
Cipher Machines
Cipher Pad
Civil Aviation Security, United States
Civil War, Espionage and Intelligence
Classified Information
Clinton Administration (1993–2001), United States National Security Policy
Clipper Chip
Closed-Circuit Television (CCTV)
Coast Guard (USCG), United States
Coast Guard National Response Center
Code Name
Code Word
Codes and Ciphers
Codes, Fast and Scalable Scientific Computation
COINTELPRO
Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Colombia, Intelligence and Security
Colossus I
COMINT (Communications Intelligence)
Commerce Department Intelligence and Security Responsibilities, United States
Commission on Civil Rights, United States
Communicable Diseases, Isolation, and Quarantine
Communications System, United States National
Comprehensive Test Ban Treaty (CTBT)
Computer and Electronic Data Destruction
Computer Fraud and Abuse Act of 1986
Computer Hackers
Computer Hardware Security
Computer Keystroke Recorder
Computer Modeling
Computer Security Act (1987)
Computer Software Security
Computer Virus
Concealment Devices
Consumer Product Safety Commission (CPSC), United States
Continuity Irish Republican Army (CIRA)
Continuity of Government, United States
Continuous Assisted Performance (CAP)
Coordinator for Counterterrorism, United States Office
Copyright Security
Counterfeit Currency, Technology and the Manufacture
Counter-Intelligence
Counter-Terrorism Rewards Program
Covert Operations
Crib
Crime Prevention, Intelligence Agencies

Critical Infrastructure
Critical Infrastructure Assurance Office (CIAO), United States
Croatia, Intelligence and Security
Cruise Missile
Cryptology and Number Theory
Cryptology, History
Cryptonym
Cuba, Intelligence and Security
Cuban Missile Crisis
Customs Service, United States
Cyanide
Cyber Security
Cyber Security Warning Network
Czech Republic, Intelligence and Security

D

D Notice
DARPA (Defense Advanced Research Projects Agency)
Data Mining
DCI (Director of the Central Intelligence Agency)
DEA (Drug Enforcement Administration)
Dead Drop Spike
Dead-Letter Box
Decontamination Methods
Decryption
Defense Information Systems Agency, United States
Defense Nuclear Facilities Safety Board, United States
Defense Security Service, United States
Delta Force
Department of State Bureau of Intelligence and Research, United States
Department of State, United States
DIA (Defense Intelligence Agency)
Dial Tone Decoder
Diplomatic Security (DS), United States Bureau
Dirty Tricks
Disinformation
DNA
DNA Fingerprinting
DNA Recognition Instruments
DNA Sequences, Unique
Document Destruction
Document Forgery
DOD (United States Department of Defense)
DOE (United States Department of Energy)
Domestic Emergency Support Team, United States
Domestic Intelligence
Domestic Preparedness Office (NDPO), United States National
Doo Transmitter
Dosimetry
Double Agents
Drop
Drug Control Policy, United States Office of National
Drug Intelligence Estimates
Dual Use Technology

E

E-2C
Ebola Virus
E-Bomb
Echelon
Economic Espionage
Economic Intelligence
Egypt, Intelligence and Security
Eichmann, Adolf: Israeli Capture
Eisenhower Administration (1953–1961), United States National Security Policy
El Salvador, Intelligence and Security
Electromagnetic Pulse
Electromagnetic Spectrum
Electromagnetic Weapons, Biochemical Effects
Electronic Communication Intercepts, Legal Issues
Electronic Countermeasures
Electronic Warfare
Electro-Optical Intelligence
Electrophoresis
EM Wave Scanners
Emergency Response Teams
Encryption of Data
Enduring Freedom, Operation
Energy Directed Weapons
Energy Regulatory Commission, United States Federal
Energy Technologies
Engraving and Printing, United States Bureau
Engulf, Operation
Enigma
Entry-Exit Registration System, United States National Security
Environmental Issues Impact on Security
Environmental Measurements Laboratory
EPA (Environmental Protection Agency)
Epidemiology
Espionage
Espionage Act of 1917
Espionage and Intelligence, Early Historical Foundations
Estonia, Intelligence and Security
European Union
Executive Orders and Presidential Directives
Explosive Coal

F

F-117A Stealth Fighter
FAA (United States Federal Aviation Administration)
Facility Security
FBI (United States Federal Bureau of Investigation)
FCC (United States Federal Communications Commission)
FDA (United States Food and Drug Administration)
Federal Protective Service, United States
Federal Reserve System, United States
FEMA (United States Federal Emergency Management Agency)
FEST (United States Foreign Emergency Support Team)

Fingerprint Analysis
Finland, Intelligence and Security
First of October Anti-fascist Resistance Group (GRAPO)
FISH (German *Geheimschreiber* Cipher Machine)
Fission
Flame Analysis
Flight Data Recorders
FM Transmitters
FOIA (Freedom of Information Act)
Food Supply, Counter-Terrorism
Ford Administration (1974–1977), United States National Security Policy
Foreign Assets Control (OFAC), United States Office
Foreign Intelligence Surveillance Act
Foreign Intelligence Surveillance Court of Review
Forensic Geology in Military or Intelligence Operations
Forensic Science
Forensic Voice and Tape Analysis
France, Counter-Terrorism Policy
France, Intelligence and Security
French Underground during World War II, Communication and Codes
Fusion

G

G–2
GAO (General Accounting Office, United States)
Gas Chromatograph-Mass Spectrometer
General Services Administration, United States
Genetic Code
Genetic Information: Ethics, Privacy and Security Issues
Genetic Technology
Genomics
Geologic and Topographical Influences on Military and Intelligence Operations
Geospatial Imagery
Germany, Counter-Terrorism Policy
Germany, Intelligence and Security
Gestapo
GIS
Global Communications, United States Office
Glomar Explorer
Government Ethics (USOGE), United States Office
GPS
Great Game
Greece, Intelligence and Security
GSM Encryption
Guatemala, Intelligence and Security
Guerilla Warfare

H

HAMAS (Islamic Resistance Movement)
Hanssen (Robert) Espionage Case
Harakat ul-Jihad-I-Islami (HUJI) (Movement of Islamic Holy War)
Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B) (Movement of Islamic Holy War)
Harakat ul-Mujahidin (HUM) (Movement of Holy Warriors)
Hardening
Health and Human Services Department, United States
Heavy Water Technology
Hemorrhagic Fevers and Diseases
Hizballah (Party of God)
Homeland Security, United States Department of
HUMINT (Human Intelligence)
Hungary, Intelligence and Security
Hypersonic Aircraft

I

IBIS (Interagency Border Inspection System)
IDENT (Automated Biometric Identification System)
Identity Theft
IFF (Identification Friend or Foe)
IMF (International Monetary Fund)
IMINT (Imagery Intelligence)
India, Intelligence and Security
Indonesia, Intelligence and Security
Infectious Disease, Threats to Security
Information Security
Information Security (OIS), United States Office of
Information Warfare
Infrared Detection Devices
Infrastructure Protection Center (NIPC), United States National
INS (United States Immigration and Naturalization Service)
INSCOM (United States Army Intelligence and Security Command)
INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)
Inspector General (OIG), Office of the
Intelligence
Intelligence Agent
Intelligence and Counterespionage Careers
Intelligence and Democracy: Issues and Conflicts
Intelligence and International Law
Intelligence and Law Enforcement Agencies
Intelligence & Research (INR), United States Bureau of
Intelligence Authorization Acts, United States Congress
Intelligence Community
Intelligence Literature
Intelligence Officer
Intelligence Policy and Review (OIPR), United States Office of
Intelligence Support, United States Office of
Intelligence, United States Congressional Oversight of
Interagency Security Committee, United States
Internal Revenue Service, United States
International Atomic Energy Agency (IAEA)
International Narcotics and Law Enforcement Affairs (INL), United States Bureau of

Internet
Internet: Dynamic and Static Addresses
Internet Spam and Fraud
Internet Spider
Internet Surveillance
Internet Tracking and Tracing
INTERPOL (International Criminal Police Organization)
Interpol, United States National Central Bureau
Interrogation
Interrogation: Torture Techniques and Technologies
Iran-Contra Affair
Iran, Intelligence and Security
Iranian Hostage Crisis
Iranian Nuclear Programs
Iraq, Intelligence and Security Agencies in
Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections)
Iraq War (Immediate Aftermath)
Iraqi Freedom, Operation (2003 War Against Iraq)
Ireland, Intelligence and Security
Irish Republican Army (IRA)
Islamic Army of Aden (IAA)
Islamic Movement of Uzbekistan (IMU)
Isotopic Analysis
Israel, Counter-Terrorism Policy
Israel, Intelligence and Security
Italy, Intelligence and Security

IJI

Jaish-e-Mohammed (JEM) (Army of Mohammed)
Japan, Intelligence and Security
Japanese Red Army (JRA)
JDAM (Joint Direct Attack Munition)
Jemaah Islamiya (JI)
Johnson Administration (1963–1969), United States National Security Policy
Joint Chiefs of Staff, United States
Jordan, Intelligence and Security
J-STARS
Justice Department, United States

IKI

Kahane Chai (Kach)
Kennedy Administration (1961–1963), United States National Security Policy
Kenya, Bombing of United States Embassy
KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)
Khobar Towers Bombing Incident
Knives
Korean War
Kosovo, NATO Intervention
Kumpulan Mujahidin Malaysia (KMM)
Kurdistan Workers' Party (PKK)
Kuwait Oil Fires, Persian Gulf War

ILI

Language Training and Skills
Laser
Laser Listening Devices
Lashkar-e-Tayyiba (LT) (Army of the Righteous)
Law Enforcement, Responses to Terrorism
Law Enforcement Training Center (FLETC), United States Federal
Lawrence Berkeley National Laboratory (LBL)
Lawrence Livermore National Laboratory (LLNL)
League of Nations
Lebanon, Bombing of U.S. Embassy and Marine Barracks
Less-Lethal Weapons Technology
L-Gel Decontamination Reagent
Liberation Tigers of Tamil Eelam (LTTE)
Libraries and Information Science (NCLIS), United States National Commission on
Libya, Intelligence and Security
Libya, U.S. Attack (1986)
LIDAR (Light Detection and Ranging)
Lock-Picking
Locks and Keys
Looking Glass
Lord Haw-Haw
Lord's Resistance Army (LRA)
Los Alamos National Laboratory
Loyalist Volunteer Force (LVF)

IMI

Mail Sanitization
Malicious Data
Manhattan Project
Mapping Technology
Marine Mammal Program
McCarthyism
Measurement and Signatures Intelligence (MASINT)
Metal Detectors
Meteorology and Weather Alteration
Mexico, Intelligence and Security
MI5 (British Security Service)
MI6 (British Secret Intelligence Service)
Microbiology: Applications to Espionage, Intelligence, and Security
Microchip
Microfilms
Microphones
Microscopes
Microwave Weaponry, High Power (HPM)
Middle East, Modern U.S. Security Policy and Interventions
Military Police, United States
MOAB (Massive Ordnance Air Burst Bomb)
Molecular Biology: Applications to Espionage, Intelligence, and Security
Moles
Monroe Doctrine
Morocco, Intelligence and Security
Mossad
Motion Sensors

Mount Weather
Movies, Espionage and Intelligence Portrayals
Mujahedin-e Khalq Organization (MEK or MKO)
Mustard Gas

N

NAILS (National Automated Immigration Lookout System)
Nanotechnology
Napoleonic Wars, Espionage during
NASA (National Air and Space Administration)
National Archives and Records Administration (NARA),Unites States
National Command Authority
National Drug Threat Assessment
National Information Infrastructure Protection Act, United States
National Intelligence Estimate
National Interagency Civil-Military Institute (NICI), United States
National Liberation Army (ELN)—Colombia
National Military Joint Intelligence Center
National Preparedness Strategy, United States
National Response Team, United States
National Security Act (1947)
National Security Advisor, United States
National Security Strategy, United States
National Security Telecommunications Advisory Committee
National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States
NATO (North Atlantic Treaty Organization)
Natural Resources and National Security
Navy Criminal Investigative Service (NCIS)
NCIX (National Counterintelligence Executive), United States Office of the
NDIC (Department of Justice National Drug Intelligence Center)
Near Space Environment
Nerve Gas
Netherlands, Intelligence and Security
New People's Army (NPA)
New Zealand, Intelligence and Security
NFIB (United States National Foreign Intelligence Board)
NIC (National Intelligence Council)
Nicaragua, Intelligence and Security
Nigeria, Intelligence and Security
Night Vision Scopes
NIH (National Institutes of Health)
NIJ (National Institute of Justice)
NIMA (National Imagery and Mapping Agency)
NIMH (National Institute of Mental Health)
NIST (National Institute of Standards and Technology), United States
NIST Computer Security Division, United States
Nixon Administration (1969–1974), United States National Security Policy
NMIC (National Maritime Intelligence Center)
NNSA (United States National Nuclear Security Administration)
NOAA (National Oceanic & Atmospheric Administration)
Noise Generators
Nongovernmental Global Intelligence and Security
Non-Proliferation and National Security, United States
NORAD
North Korea, Intelligence and Security
North Korean Nuclear Weapons Programs
Norway, Intelligence and Security
NRO (National Reconnaissance Office)
NSA (United States National Security Agency)
NSC (National Security Council)
NSC (National Security Council), History
NSF (National Science Foundation)
NTSB (National Transportation Safety Board)
Nuclear Detection Devices
Nuclear Emergency Support Team, United States
Nuclear Power Plants, Security
Nuclear Reactors
Nuclear Regulatory Commission (NRC), United States
Nuclear Spectroscopy
Nuclear Weapons
Nuclear Winter
Nucleic Acid Analyzer (HANAA)

O

Oak Ridge National Laboratory (ORNL)
Official Secrets Act, United Kingdom
OPEC (Organization of Petroleum Exporting Countries)
Operation Liberty Shield
Operation Magic
Operation Mongoose
Operation Shamrock
Orange Volunteers (OV)
OSS (United States Office of Strategic Services)

P

P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft
Pacific Northwest National Laboratory
Pakistan, Intelligence and Security
Palestine Islamic Jihad (PIJ)
Palestine Liberation Front (PLF)
Palestinian Authority, Intelligence and Security
PanAm 103, (Trial of Libyan Intelligence Agents)
Panama Canal
Parabolic Microphones
Pathogen Genomic Sequencing
Pathogen Transmission
Pathogens
Patriot Act Terrorist Exclusion List
Patriot Act, United States
Patriot Missile System
Pearl Harbor, Japanese Attack on
People Against Gangsterism and Drugs (PAGAD)
Persian Gulf War
Peru, Intelligence and Security

Petroleum Reserves, Determination
PFIAB (President's Foreign Intelligence Advisory Board)
Phoenix Program
Photo Alteration
Photographic Interpretation Center (NPIC), United States National
Photographic Resolution
Photography, High-Altitude
Playfair Cipher
Plum Island Animal Disease Center
Poland, Intelligence and Security
Politics: The Briefings of United States Presidential Candidates
Pollard Espionage Case
Polygraphs
Polymerase Chain Reaction (PCR)
Popular Front for the Liberation of Palestine (PFLP)
Popular Front for the Liberation of Palestine-General Command (PFLP-GC)
Port Security
PORTPASS (Port Passenger Accelerated Service System)
Portugal, Intelligence and Security
Postal Security
Postal Service (USPS), United States
Potassium Iodide
President of the United States (Executive Command and Control of Intelligence Agencies)
Pretty Good Privacy (PGP)
Privacy: Legal and Ethical Issues
Profiling
Propaganda, Uses and Psychology
Pseudoscience Intelligence Studies
Psychotropic Drugs
Public Health Service (PHS), United States
Pueblo Incident
Purple Machine

Q

Quantum Physics: Applications to Espionage, Intelligence, and Security Issues

R

RADAR
RADAR, Synthetic Aperture
Radiation, Biological Damage
Radio Direction Finding Equipment
Radio Frequency (RF) Weapons
Radioactive Waste Storage
Radiological Emergency Response Plan, United States Federal
Reagan Administration (1981–1989), United States National Security Policy
Real IRA (RIRA)
Reconnaissance
Red Code
Red Hand Defenders (RHD)
Red Orchestra
Remote Sensing
Retina and Iris Scans
Revolutionary Armed Forces of Colombia (FARC)
Revolutionary Nuclei
Revolutionary Organization 17 November (17 November)
Revolutionary People's Liberation Party/Front (DHKP/C)
Revolutionary Proletarian Initiative Nuclei (NIPR)
Revolutionary United Front (RUF)
Revolutionary War, Espionage and Intelligence
RF Detection
Ricin
Robotic Vehicles
Romania, Intelligence and Security
Room 40
Rosenberg (Ethel and Julius) Espionage Case
Russia, Intelligence and Security
Russian Nuclear Materials, Security Issues

S

Sabotage
Salafist Group for Call and Combat (GSPC)
Salmonella and Salmonella Food Poisoning
Sandia National Laboratories
Sarin Gas
Satellite Technology Exports to the People's Republic of China (PRC)
Satellites, Non-Governmental High Resolution
Satellites, Spy
Saudi Arabia, Intelligence and Security
Scanning Technologies
SEAL Teams
Secret Service, United States
Secret Writing
Security Clearance Investigations
Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator
Security Policy Board, United States
Seismograph
Seismology for Monitoring Explosions
Senate Select Committee on Intelligence, United States
Sendero Luminoso (Shining Path, or SL)
SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)
September 11 Terrorist Attacks on the United States
Sequencing
Serbia, Intelligence and Security
Sex-for-Secrets Scandal
Ships Designed for Intelligence Collection
"Shoe Bomber"
Shoe Transmitter
Short-Wave Transmitters
SIGINT (Signals Intelligence)
Silencers
Skunk Works
Slovakia, Intelligence and Security
Slovenia, Intelligence and Security
Smallpox
Smallpox Vaccine

SOE (Special Operations Executive)
Soldier and Biological Chemical Command (SBCCOM), United States Army
Solid-Phase Microextraction Techniques
Soman
SONAR
SOSUS (Sound Surveillance System)
South Africa, Intelligence and Security
South Korea, Intelligence and Security
Soviet Union (USSR), Intelligence and Security
Space Shuttle
Spain, Intelligence and Security
Spanish-American War
Special Collection Service, United States
Special Counsel and Security Related "Whistleblower" Protection Issues, United States Office
Special Operations Command, United States
Special Relationship: Technology Sharing between the Intelligence Agencies of the United States and United Kingdom
Spectroscopy
Spores
SR-71 Blackbird
START I Treaty
START II
STASI
Stealth Technology
Steganography
Strategic Defense Initiative and National Missile Defense
Strategic Petroleum Reserve, United States
Sudan, Intelligence and Security
Suez Canal
Supercomputers
Surgeon General and Nuclear, Biological, and Chemical Defense, United States Office
Sweden, Intelligence and Security
Switzerland, Intelligence and Security
Syria, Intelligence and Security

T

Tabun
Taiwan, Intelligence and Security
Taser
Technical Intelligence
Technology Transfer Center (NTTC), Emergency Response Technology Program
Telemetry
Telephone Caller Identification (Caller ID)
Telephone Recording Laws
Telephone Recording System
Telephone Scrambler
Telephone Tap Detector
Terror Alert System, United States
Terrorism, Domestic (United States)
Terrorism, Intelligence Based Threat and Risk Assessments
Terrorism, Philosophical and Ideological Origins
Terrorism Risk Insurance
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets
Terrorist Threat Integration Center
Thin Layer Chromatography
TIA (Terrorism Information Awareness)
Tissue-Based Biosensors
Tokyo Rose
Toxicology
Toxins
Tradecraft
Transportation Department, United States
Treasury Department, United States
Truman Administration (1945–1953), United States National Security Policy
Truth Serum
Tularemia
Tunisian Combatant Group (TCG)
Tupac Amaru Revolutionary Movement (MRTA)
Turkey, Intelligence and Security
Turkish Hizballah
Typex

U

U-2 Incident
U-2 Spy Plane
Ukraine, Intelligence and Security
Ulster Defense Association/Ulster Freedom Fighters (UDA/UVF)
Ultra, Operation
Underground Facilities, Geologic and Structural Considerations in the Construction
Undersea Espionage: Nuclear vs. Fast Attack Subs
Unexploded Ordnance and Mines
United Kingdom, Counter-Terrorism Policy
United Kingdom, Intelligence and Security
United Nations Security Council
United Self-Defense Forces/Group of Colombia (AUC *Autodefensas Unidas de Colombia*)
United States, Counter-Terrorism Policy
United States, Intelligence and Security
United States Intelligence, History
Unmanned Aerial Vehicles (UAVs)
Uranium
Uranium Depletion Weapons
USAMRICD (United States Army Medical Research Institute of Chemical Defense)
USAMRIID (United States Army Medical Research Institute of Infectious Diseases)
USS *Cole*
USS *Liberty*
USSTRATCOM (United States Strategic Command)

V

Vaccination
Vaccines
Variola Virus
Venezuela, Intelligence and Security
Venona
Vietnam War
Viral Biology

Viral Exposure Therapy, Antiviral Drug Development
Voice Alteration, Electronic
Voice of America (VOA), United States
Vozrozhdeniye Island, Soviet and Russian Biochemical Facility
Vulnerability Assessments
VX Agent

W

Walker Family Spy Ring
War of 1812
Water Supply: Counter-Terrorism
Watergate
Weapon-Grade Plutonium and Uranium, Tracking
Weapons of Mass Destruction
Weapons of Mass Destruction, Detection
Windtalkers
World Health Organization (WHO)
World Trade Center, 1993 Terrorist Attack
World Trade Center, 2001 Terrorist Attack
World War I
World War I: Loss of the German Codebook
World War II
World War II: Allied Invasion of Sicily and "The Man Who Never Was"
World War II, The Surrender of the Italian Army
World War II, United States Breaking of Japanese Naval Codes

Z

Zoonoses

This page intentionally left blank

R

RADAR

LARRY GILMAN

RADAR—an acronym for RAdio Detection And Ranging—is the use of electromagnetic waves at sub-optical frequencies (i.e., less than about 10^{12} Hz) to sense objects at a distance. Hundreds of different RADAR systems have been designed for various purposes, military and other. RADAR systems are essential to the navigation and tracking of craft at sea and in the air, weather prediction, and scientific research of many kinds.

Principles. In basic RADAR, radio waves are transmitted from an antenna. These outgoing waves eventually bounce off some distant object and return an echo to the sender, where they are received, amplified, and processed electronically to yield an image showing the object's location. The waves sent out may be either short oscillatory bursts (pulses) or continuous sinusoidal waves. If a RADAR transmits pulses it is termed a pulse RADAR, whereas if it transmits a continuous sinusoidal wave it is termed a continuous-wave RADAR.

On closer examination, the RADAR process is seen to be more complex. For example, reflection of an echo by the object one wishes to sense is anything but straightforward. Upon leaving a transmitting antenna, a radio wave propagates in a widening beam at the speed of light (> 186,000 miles per hour [3×10^8 m/sec]); if it encounters an obstacle (i.e., a medium whose characteristic impedance differs from that of air and vacuum [> 377 Ω), it splits into two parts. One part passes into the obstacle and is (generally) absorbed, and the other is reflected. Where the reflected wave goes depends on the shape of the obstacle. Roundish or irregular obstacles tend to scatter energy through a wide angle, while flat or facet-like surfaces tend to send it off in a single direction, just as a flat mirror reflects light. If any part of the outgoing wave is reflected at 180° (which is not guaranteed) it will return to the transmitter. This returned or backscattered signal is usually detected by the same antenna that sent the outgoing pulse; this antenna alternates rapidly between transmitting pulses and listening for echoes, thus building a real-time picture of the reflecting targets in range of its beam. The energy the echoes receive is a small fraction of that in the pulses transmitted, so the strength of the transmitted pulse and the sensitivity of the receiver determines a RADAR's range. By systematically sweeping the direction in which its antenna is pointed, a RADAR system can scan a much larger volume of space than its beam can interrogate at any one moment; this is why many RADAR antennas, on ships or atop air-traffic control towers, are seen to rotate while in operation.

Radio waves are not the only form of energy that can be used to derive echoes from distant targets. Sound waves may also be used. Indeed, because radio waves are rapidly absorbed in water, sonar (SOund Navigation and Ranging) is essential to underwater operations of all sorts, including sea-floor mapping and anti-submarine warfare.

Applications. Since World War II RADAR has been deployed in many forms and has found a wide application in scientific, commercial, and military operations. RADAR signals have been bounced off targets ranging in size from dust specks to other planets. RADAR is essential to rocketry and early-warning detection of missiles, air traffic control, navigation at sea, automatic control of weapons such as antiaircraft guns, aircraft detection and tracking, mapping of the ground from the air, weather prediction, intruder detection, and numerous other tasks. Few craft, military or civilian, put to sea or take to the air without carrying some form of RADAR.

In recent decades, development of the basic RADAR principle—send pulse, listen for echo—has proceeded along a number of interesting paths. By exploiting the Doppler effect, which causes frequency shifts in echoes reflected from moving objects, modern RADARs can tell not only where an object is but what direction it is moving

in and how quickly. The Doppler effect also allows for the precision mapping of landscapes from moving aircraft through the synthetic-aperture technique. Synthetic-aperture systems exploit the fact that stationary objects being swept by a RADAR beam projected from a moving source have, depending on their location, slightly different absolute velocities with respect to that source. By detecting these velocity differences using the Doppler effect, synthetic aperture type RADAR greatly permits the generation of high-resolution ground maps from small, airborne RADARs.

In many modern RADAR systems the need for a mechanically moving antenna has been obviated by phased arrays. A phased array consists of a large number of small, computer-controlled antennas termed elements. These elements, of which there are usually thousands, are crowded together to form a flat surface. In transmit mode, the elements are all instructed to emit a RADAR pulse at approximately the same time; the thousands of outbound waves produced by the elements merge into a single powerful wave as they spread outward. By timing, or *phasing,* the elements in the array so that, for example, elements along the left-hand edge of the array fire first while those farther to the right fire progressively later, the composite wave formed by the merging of the elements' lesser outputs can be steered in any desired direction within a wide cone (in this example, to the right). Beam steering can be accomplished by such a system millions of times more rapidly than would be possible with mechanical methods. Phased-array systems are used for a number of applications; including the 71.5-foot (21.8-m) tall AN/FPS-115 PAVE PAWS Early Warning RADAR Array Antennas, which provide early warning of ballistic-missile attack; shipboard systems such as the AN/SPY-1D, which is about 15 feet (3 m) across and is mounted flush with the upper hull of some warships; the Hughes AN/TPQ-37 Firefinder, a trailer-mounted system designed for tracking incoming artillery and missiles and calculating their point of origin; and many other real-world systems.

RADAR is a powerful weapon of war, but has its weaknesses. For example, numerous missiles have been developed to home in on the radio pulses emitted by RADARs, making it very dangerous to turn on a RADAR in a modern battlefield situation. Further, jamming and spoofing ("electronic warfare") have evolved rapidly alongside RADAR itself. For example, an aircraft that finds itself interrogated by a RADAR pulse can emit blasts of noise or false echoes, or request that a drone or other unit emit them, in order to confuse enemy RADAR. Finally, aircraft have been built that are "low observable," that is, which scatter very little energy back toward any RADAR that illuminates them. Low-observable or "stealth" aircraft are built of radio-absorbent materials and shaped to present little or no surface area perpendicular to RADAR pulses approaching from most angles (except directly above and directly below, the two least likely places for an enemy RADAR to be at any given moment). What RADAR they do reflect is deflected at low angles rather than returned to the RADAR transmitter. The U.S. B-2 bomber and F-117A and F-22 fighters are working examples of low-observable aircraft.

FURTHER READING:

BOOKS:

Edde, Byron. *RADAR: Principles, Technology, Applications.* Englewood Cliffs, NJ: PTR Hall, 1993.

Skolnik, Merrill I. *Introduction to RADAR Systems.* New York: McGraw Hills, 2001.

SEE ALSO

Stealth Technology
RADAR, Synthetic Aperture

RADAR Detection Avoidance.

SEE *Stealth Technology.*

RADAR, Synthetic Aperture

Synthetic aperture RADAR (SAR) is used for high-resolution mapping of the ground from moving aircraft or spacecraft. A stationary RADAR system's angular resolution—that is, the clarity with which it can distinguish two small, side-by-side targets at a given distance—is determined by the physical width (aperture) of its antenna. By appropriate processing of the echoes received by a small, but moving antenna, an angular resolution equivalent to that of a much larger antenna can be synthesized—hence the term "synthetic aperture RADAR" for such a system.

SAR exploits the Doppler effect, a property of waves reflected (or emitted) by moving objects. If a wave is reflected or emitted by an object approaching a receiver, its frequency as perceived by the receiver is raised; if the object is receding, its frequency is perceived by the receiver as lowered. Most people have noticed the Doppler effect when a vehicle blowing its horn passes them at high speed; the sound of the horn is high-pitched when the vehicle is approaching, then drops when the vehicle passes by. Basic SAR works as follows: first, a narrow, fan-shaped radar beam is projected at right angles to the forward motion of an aircraft (or other platform). Distant objects cut across this side-looking beam as the aircraft moves in a straight line. As an object first enters the beam, its relative motion has a component that is toward the aircraft and which Doppler-shifts its RADAR reflection to higher frequencies. As the object passes through the centerline of the beam, it ceases to get closer to the aircraft. At this fraction of a second, its reflection ceases to be Doppler shifted. Next, as the object passes through the trailing half

of the beam, it begins to move away from the aircraft, which Doppler-shifts its reflection to lower frequencies. Thus, although reflections from all objects at a given distance from the RADAR return to its antenna at the same moment, reflections from objects ahead of the aircraft are Doppler shifted to higher frequencies, and those from objects trailing the aircraft are shifted to lower frequencies. This effect can be used to distinguish objects inside the beam, achieving an angular resolution that is higher than the beam's physical width.

SAR mapping was first demonstrated in 1953 and has since been widely used by the military (with various refinements) for airborne battlefield surveillance. SAR has also been used for satellite-based radar mapping of the Earth and Venus.

FURTHER READING:

BOOKS:

Edde, Byron. *RADAR: Principles, Technology, Applications.* Englewood Cliffs, NJ: PTR Prentice Hall, 1993.

Fitch, J. Patrick. *Synthetic Aperture RADAR.* West Hanover, MA: Springer-Verlag, 2001.

SEE ALSO

RADAR

Radiation, Biological Damage

ABDEL HAKIM BEN NASR
BRIAN HOYLE

The nuclear explosions at Hiroshima and Nagasaki, Japan on August 6 and 9, 1945, demonstrated the immense power of the nuclear bomb. The effects of the explosion were immediate. The radiation that was released by the explosions, however, caused the deaths of many people weeks, months, and even years later. It is this radiation-induced biological damage that can ultimately claim more lives than those lost in the blast of a nuclear weapon.

Radiation released in a nuclear explosion consists of particles that have a high energy. When these particles encounter biological material, in particular deoxyribonucleic acid (DNA), they can break the DNA strands. The breakage can be so severe that a cell's repair machinery cannot compensate. Because DNA is the blueprint for the structure and all the activities that occur in cells, the radiation-induced damage to DNA is lethal to the affected cells.

Radiation exposure that does not kill cells outright can cause sublethal damage that scrambles the sequence of information contained in the DNA. As a result, when the DNA is used to make proteins, proteins that are altered from the intended forms will be made. These represent mutations.

Mutations occur naturally at a very low rate. Using special agents called mutagens can increase the frequency of these mutations. Ionizing radiation was the first mutagen that efficiently and reproducibly induced mutations in a multicellular organism. Radiation is often classified as ionizing or non-ionizing depending on whether ions are emitted in the penetrated tissues or not. Examples of ionizing radiation include x rays, gamma rays, beta particle radiation, and alpha particle radiation (also known as alpha rays). The ultraviolet radiation that is a component of sunlight is an example of a nonionizing radiation.

Different types of radiation have different energies, and so have different effects. With alpha radiation, ionizations produce an intense but more superficial and localized deposition of energy. The energy of x rays and gamma radiation traverses deeper into tissues. This penetration leads to a more even distribution of energy as opposed to the more concentrated or localized alpha rays.

The different behaviors of different types of radiation can be used to some extent to tailor the radiation to selected cellular components. Experiments conducted on animals have shown that repeated exposure to radiation produces a higher frequency of mutations than a single exposure to a higher level of radiation. In other words, exposure to a low level of radiation can be damaging over time.

The relative efficiencies of the different types of radiation in producing mutations can be compared, and is known as the mutagenic effect. Investigation of radiation's mutagenic effects on different tissues, cells, and subcellular compartments is becoming possible by the availability of techniques and tools that allow the precise delivery of small doses of radiation and that provide better monitoring of effects.

Cells that are irradiated release a form of oxygen that is unstable, and which reacts with cellular components in a way that is damaging. DNA can be damaged, as can components called bases, which are assembled to form DNA strands. As well, the reactive oxygen can damage enzymes that function to repair damaged DNA. There is evidence that radiation damage in one cell can be passed on to neighbouring cells. Even the neighbouring cells may be damaged genetically. Thus, radiation damage, especially due to low levels of radiation, may be more extensive than previously assumed.

This increased risk of radiation damage is of concern, as terrorist organizations such as al Qaeda have made efforts to develop and deploy "dirty bombs"—conventional explosives that release a payload of radioactive material. In 2002, an American citizen was arrested for his alleged involvement with al Qaeda to detonate a dirty bomb inside the United States. The spray of radiation in a mid-level dirty bomb could produce a relatively low level of radiation over a fairly localized area. In a densely-populated city, thousands of people could be exposed to

harmful levels of radiation from an explosion from a dirty bomb.

■ FURTHER READING:

BOOKS:

Cheung, Kin P. *Plasma Charging Damage.* Berlin: Springer Verlag, 2000.

Mangano, Joseph, J. *Low level radiation and Immune System Damage: An Atomic Era Legacy.* Boca Raton: Lewis Publishers, 1998.

PERIODICALS:

Azzam, E. I., S. M. de Toledo, and J. B. Little. "Direct evidence for the participation of gap junction-mediated intercellular communication in the transmission of damage signals from alpha-particle irradiated to nonirradiated cells." *Proceedings of the National Academy of Sciences* no. 98 (2001): 473–478.

SEE ALSO

Nuclear Detection Devices
Weapons of Mass Destruction, Detection

Radio Direction Finding Equipment

One of the earliest military applications for radio was in direction-finding (DF), which makes it possible to locate the positions of enemy aircraft and ships using four major components: an antenna, a receiver, a processor or processors, and a control and output system. Examples of radio DF equipment in use at the beginning of the twenty-first century include the OUTBOARD (Organizational Unit Tactical Baseline Operational Area Radio Detection) system of the U.S. Navy. Direction finding often uses triangulation, which is based on laws of plane trigonometry.

Direction finding and triangulation. A direction finder can be any electronic device used to locate a source of electronic emissions such as a ship or aircraft. In everyday usage by military, security, and intelligence services, direction finding is virtually synonymous with radio DF. Direction finding usually involves a radio receiver linked to a revolving antenna, which scans for the strongest possible signal in the area.

Assuming two stationary transmitters can be located, direction finding can be used to locate one's position by means of triangulation. The latter is based on the trigonometric principle that, for any triangle, when one side and two angles are known, the other angle and two sides can be calculated. To establish the measure for two angles of a triangle on Earth's surface, it is necessary to use a surveying device known as a theodolite, or some electronic equivalent. The measured and known side of the triangle is known as the baseline.

Components of a DF system. The simplest DF system must contain an antenna, receiver, at least one processor, and control/output systems. The antenna must be versatile, so as to address a variety of requirements, some of which seem almost at cross-purposes to one another. It must be omnidirectional, or capable of receiving input from 360 degrees, yet capable of pinpointing the locations of specific signals from the range of radio noise it receives. Additionally, it must make possible the reception of signals over the widest possible area, yet receive these on an ultra-accurate pencil beam. Given these various requirements, modern DF systems often use not one antenna but an array, or they may make use of a phased-array antenna, which can quickly change its pattern of radiation using electronic means.

Receivers may be either single-channel, dual-channel, or N-channel. In a single-channel receiver, a switch sequentially selects one antenna from an array, while in the dual-channel model, switching may be used to select pairs from three or more antennas. N-channel receivers are capable of operating across multiple antennas without the requirement of switching.

Once the signal is received, it is necessary to calculate the location of the emitter by comparing signal properties such as amplitude. For this operation, a processor is used. With multiple or phased-array antennas, the operator may need not a single processor, but an array of distributed digital signal processors. With twenty-first century technology, it is possible for machines to perform a variety of complex calculations in real time or near-real time. Lastly, there is the control/output system, which includes a variety of subcomponents such as functions for the input and preparation of data, as well as various other operations requiring a workable interface between operator and equipment.

Radio DF in history. The use of radio direction finding dates back to World War I, when both the Allies and the forces of the Central Powers used it to locate enemy positions on the ground. The essential principles of direction-finding were established at that time, well before radio entered commercial use in the early 1920s.

During the interwar period, the British Royal Navy used radio DF extensively with the aid of listening stations. The latter had been established in the wake of escalating international conflicts, including the Italian invasion of Ethiopia (which potentially threatened British-controlled lands in east Africa) and the Spanish Civil War,

during which Italian submarines threatened British vessels transporting supplies to Republican forces.

By the late 1930s, the British had begun using high-frequency direction finding (HF/DF or "Huff Duff") equipment on their warships. This technology had benefited from improvements by Canadian engineers, who created a means of automatically recording the directional bearings of transmissions by radio. During the Second World War, the Royal Navy successfully used HF/DF to locate German submarines in the north Atlantic.

Across the ocean, the U.S. Navy received help from French scientists who had escaped the Nazi and Vichy regimes, and who assisted Navy technicians in developing a means of visual imaging to record the bearings of a vessel emitting transmissions. This equipment, tested in 1940 and operational by the latter part of 1942, also made it possible to maintain a track on an enemy U-boat even after the latter had stopped transmitting.

DF in the Cold War and modern era. The Germans themselves made advances in antenna technology, but because of their failure to accurately assess Allied DF capabilities, the principal beneficiaries of these developments would later be their wartime adversaries. During the 1950s and 1960s, the U.S. military adapted German Wullenweber antenna systems for use in Vietnam and other theatres of the Cold War. The United States also made used of the Wullenwebers (sometimes referred to as circularly disposed dipole antenna arrays or CDDAs) for land-based electronic eavesdropping, taking advantage of their wide operational range of 3,200 miles (5,150 km). Today, abandoned Wullenwebers—nicknamed "rings of poles," "dinosaur cages," or "elephant cages"—dot the globe, an almost poignant visual symbol of the long-vacated superpower conflict.

At the turn of the twenty-first century, radio DF equipment was a standard feature of U.S. Navy vessels. By 2000, the OUTBOARD system had been in use on naval vessels for many years, and was slated for an upgrade through the Cooperative OUTBOARD Logistics Update (COBLU) program. OUTBOARD made use of high-frequency deck-edge antennas and VHF (very high frequency) mast antennas, as well as a receiver that automatically searched for, received, collected, and analyzed signals. Thus, it combined the receiving and processing functions in a single piece of equipment. Its control/output system is capable of collecting processed cryptologic transmissions and transmitting intelligence to other members of the battle group via data links.

FURTHER READING:

PERIODICALS:

Cochran, William W. "Direction Finding at Ultra High Frequency (UHF): Improved Accuracy." *Wildlife Society Bulletin* 29, no. 2 (summer 2001): 594.

ELECTRONIC:

Herskovitz, Don. "A Sampling of Direction-Finding Systems." *Journal of Electronic Defense* 23, no. 8 (August 2000): 57–65.

Rivers, Brendan. "U.S. Navy Orders OUTBOARD Update." *Journal of Electronic Defense* 23, no. 8 (August 2000): 31.

Robinson, Clarence O., Jr. "Position-Fixing Methods Use Broadband Direction Finders." *Signal* 53, no. 2 (October 1998): 71–74.

SEE ALSO

Electronic Countermeasures
Electronic Warfare
FM Transmitters
GPS
SIGINT (Signals Intelligence)

Radio Frequency (RF) Weapons

RF, or radio frequency weapons, also known as directed-energy weapons, use electromagnetic energy on specific frequencies to disable electronic systems. The principle is similar to that of high-power microwave (HPM) weapons, only HPM systems tend to be much more sophisticated, and are thus, more likely to be in the control of superpowers or near-superpowers. RF weapons, by contrast, are simple and low-voltage enough that they could be deployed by smaller, less technologically enhanced forces.

The range of frequencies for waves in the electromagnetic spectrum is from approximately 10^2 Hz to more than 10^{25} Hz—in other words, from about 100 cycles per second to about 10 trillion trillion. From the lowest frequencies to about 10^{10} Hertz is the range of long-wave radio, shortwave radio, and microwaves. These carry broadcast radio, television, mobile phone communications, radar, and even highly specific forms of transmission such as those of baby monitors or garage-door openers.

Because of regulation by the Federal Communications Commission (FCC), AM or amplitude modulation broadcasts take place across a frequency range from 535 kHz (kilohertz, or 1,000 Hertz) to 1.7 MHz (megahertz, or 1,000,000 Hertz). The FCC has assigned the range of 5.9 to 26.1 MHz to shortwave radio, and 26.96 to 27.41 MHz to citizens' band (CB) radio. Above these are microwave regions assigned to very high frequency (VHF) television stations 2 through 6, then FM (frequency modulation) radio, which occupies the range from 88 to 108 MHz. Higher still are VHF channels 7 to 13, ultra-high frequency (UHF) television broadcasts, and so on. At the highest

microwave ranges—around 10^{10} Hz—are transmissions from spacecraft.

FCC regulation is necessary to maintain security, privacy, and safety on the airwaves. If a broadcaster or receiver strays outside of its assigned range, it can intercept private communications, or potentially disrupt highly sensitive transmissions. Among the most sensitive from a safety perspective, are the communications between an aircraft cockpit and the control tower, which could result in serious consequences if disrupted even for a few seconds.

High-power microwave weaponry is of such voltage and intensity that it can actually shut off the computer systems of an aircraft long enough that a pilot could conceivably be unable to right the craft, causing a crash. With an RF weapon, the intensity of the signal is smaller, but if properly directed, it could potentially disrupt aircraft communication systems long enough to bring down the craft. It could cause the computers to reset, or disrupt safety sensors, navigation systems, data recorders, or control systems. Enough errors in these sensitive flight components, particularly in the highly computerized aircraft of today, might be enough to force a plane out of the sky.

Concerns over RF interference dictate the prohibition against cell phone, radio, or even laptop computer operation aboard a plane from the time of preparation for takeoff until after it lands. Such relatively weak and innocuous systems could interfere with vital flight communications; one can easily imagine the harm that could be done by terrorists operating a directed and more powerful system with malicious intent. Adding to the dangers of RF weaponry is the fact that it could potentially be operated from the ground, allowing the terrorist to attack and seek cover in the process, and rendering the sacrifice of the terrorist's life unnecessary. Furthermore, RF weaponry, like most means of electromagnetic warfare, is "clean," meaning that, unlike ordinary ballistic weaponry, it is almost untraceable.

FURTHER READING:

PERIODICALS:

Larson, Virgil. "The Next Wave: Using Radio Frequency as Weapon." *Omaha World-Herald.* (April 14, 2002): 1D.

"Moscow, Tehran to Discuss RF Weapons Supplies to Iran—VP." *Itar-Tass News Wire.* (February 28, 2001): 1.

"Russia Developing New Radio Frequency Weapons." *Electromagnetic News Report* 30, no. 2 (March/April 2002): 1.

SEE ALSO

E-Bomb
Electromagnetic Pulse
Electronic Countermeasures
Electronic Warfare
Microwave Weaponry, High Power (HPM)

Radioactive Waste Storage

ADRIENNE WILMOTH LERNER

The storage of radioactive waste generated by the use and production of radioactive materials within the United States remains a contentious national security issue. The security of these materials, many taking thousands of years to decay, requires not only security measures to prevent tampering or theft, but also important considerations of the physical environment of waste storage. Site selection must ultimately be based upon minimizing the potential for leakage and long-term environmental damage.

In the 1960s, nuclear power gained popularity as a means of producing electricity for civilian use. During the next two decades, several nuclear power plants were built, but there was little consensus about how to best dispose of radioactive waste. Waste from plants, as well as from military and defense operations, was usually stored on site or in nearby storage facilities. Low-level waste, such as that from hospitals, research labs, and power plants is generally placed into containment facilities on-site. However, the disposal of high-level waste, materials that are highly radioactive, remains more problematic. Spent nuclear fuels from power plants are sometimes shipped to containment facilities, and sometimes stored in specially constructed containment pools on-site. Radioactive waste is thus, stored in various locations, governed by federal regulations. Forty-three states in the United States, and several Canadian provinces, currently have nuclear waste storage facilities. In the late 1990s, the government proposed plans for a central storage facility for high-level waste at Yucca Mountain, Nevada. In May, 2002, the United States House of Representatives approved a measure that would establish the site at Yucca Mountain, and approval was pending as of June 2002. The proposed site has sparked ongoing controversy over the environmental impact of nuclear waste storage, much of which focuses on the unique geological and environmental conditions of the region.

When looking for a site for permanent storage of high level waste, engineers and geologists took several factors into consideration, including: water table, geological stability, rock composition, seismic (earthquake) activity, and proximity to population areas. Furthermore, the site must have a high probability of remaining undisturbed for tens of thousands of years, or as long as the materials in storage are radioactive. Yucca Mountain is located in a rural region, with sparse population. Las Vegas, 100 miles (160 km) from the site, is the nearest metropolitan area. Within a 100-mile radius of the proposed site, there are approximately 35,000 inhabitants. Thus, Yucca Mountain is relatively secluded.

Yucca Mountain itself has a desert climate, receiving less than six inches of rain per year. The lack of rain means that cave systems within the mountain are dry, and that

there is minute seepage from the surface of the mountain to the deep water table 2000 feet (670 meters) below ground. This ensures that waste stored in the mountain would have fewer chances of polluting ground water if specially engineered storage containers ever rupture. The deep location of the water table at the site also means that the cavity, or storage room, would lie equidistant from the surface of the mountain to ground water stores—about 1000 feet, or 304 meters. This isolates the waste, and removes the chance of accidental disturbance from future drilling or other means of exploration.

Some aspects of the geological composition of the mountain itself further makes Yucca Mountain a candidate for a nuclear waste repository. Dense volcanic rock, as well as thick and nearly impenetrable bedrock mean Yucca Mountain's interior is relatively stable, not very porous, and resistant to water and heat. Under the most extreme conditions, this deep and solid rock could help contain minor seepage, as well as insulate the repository—possibly making it as safe as a band of untapped uranium ore.

Yucca Mountain's unique geology and environment is unequaled by that of any of the nation's other current nuclear waste repositories, many of which pose a greater potential threat to cities, drinking water, and their local environments. Centralization could potentially lead to tighter regulation of waste, better handling, and less environmental damage.

While Yucca Mountain does meet much of the criteria for a safe storage site, it is not a perfect location. The region around Yucca Mountain contains several faults and fractures (cracks in the Earth's crust where movement causes earthquakes), and is considered seismically active. Earthquakes could change the patterns of water flow inside the mountain, as well as endanger the integrity of the storage cavities within the mountain. Increased hydrothermal activity could promote seepage and water contamination.

Researchers also explored the possibility of the storage cavity filling with water, thus exposing the aquifer and groundwater to radioactive contaminants. Geologists studied core samples and cave linings to determine the extent to which minerals permeated the walls of the cavities. The scientists found that there were only scant traces of opal and calcite, telltale signs of flooding and water seepage, at the lower levels of the mountain. Thus, the cavities did not have a history of filling with water. A corresponding study of the geological history of the mountain further confirmed the relative stability of the site's water table, drainage, and seepage.

However, under Yucca Mountain is a deep aquifer. In the desert region, the aquifer provides drinking and irrigation water. As metropolitan centers, such as Las Vegas, continue to grow, the aquifer might play a significant role as a water resource for the region. The nuclear storage site would have to remain stable and well sealed for tens of thousands of years in order to insure the continued safety of the aquifer.

Part of the problem in designing high-level waste storage facilities is the time span for which these sites must remain secure and safe. Lab tests are inadequate to insure the stability of the mountain, the fortitude of containers and casks, and the security of the site from accidental intrusion for the tens of thousands of years necessary for radioactive waste to be rendered harmless. Project planners face not only design difficulties such as preventing accidents and mitigating environmental impact, but also how to document the site in ways that will ensure that people 10,000 years from now will recognize the hidden danger of the mountain storage facility. People today have only scant artifacts and generalized understanding of civilizations and people that lived ten thousand years ago.

Geologists and other scientists disagree on the possible effect that the waste could have on the behavior of the mountain itself. Some predict that heat generated by the waste could alter the mountain's geological and hydrological behavior, causing rocks to crack and water to seep into and out of the storage cavity in ways that we cannot predict. Some raise concerns over the unpredictable nature of seismic activity in the area. Other scientists assert that the stable pattern of geological processes at Yucca Mountain will remain unchanged, and that the site is predictably stable. Geologists have to account for not only the mountain's history, but also predict its future in order to insure the safety of the site for future generations.

While much of the scientific community's assessment of the safety of the Yucca Mountain project centers on geology, public concerns focus on technology. Though waste is currently stored in forty-three states, little of the nation's spent nuclear materials travel long distances. The creation of the Yucca Mountain site would require that waste be shipped by truck and rail to the central storage facility. Engineers and researchers have developed safe casks, or storage bins, which are impervious to accidents, water, and fire specifically for shipping high-level waste, but may people are discomforted simply by the perceived risk (the threat that people feel is associated with a given project, not the statistical risk) of shipping nuclear materials.

The controversy surrounding the proposed Yucca Mountain waste repository is both political and scientific. The perceived threat of nuclear materials heavily influences public opinion, and environmentalists are reticent to trade many smaller environmental problems for a large potential hazard. Some people cite the Yucca Mountain facility as a means of centralizing the problem of nuclear waste. Project proponents claim that the repository will lessen environmental risk and keep volatile, dangerous materials secure and controlled.

FURTHER READING:

BOOKS:

Bechthold, W., et al. *Direct Disposal of Spent Nuclear Fuel (Radioactive Waste Management Series).* N.p., Graham & Trotman, 1988.

Hafner, R. S., ed. "Transportation, Storage, and Disposal of Radioactive Materials: Presented at the 1999 *Asme Pressure Vessels and Piping Conference.*" American Society of Mechanical Engineers, 1990.

SEE ALSO

NNSA (United States National Nuclear Security Administration)
Nuclear Power Plants, Security
Nuclear Reactors

Radiological Emergency Response Plan, United States Federal

The Federal Radiological Emergency Response Plan (FRERP) is a blueprint for the response of the United States federal government to a radiological emergency—that is, a crisis involving the release of nuclear radiation. Drafted by a Federal Emergency Management Agency (FEMA) committee in 1985, FRERP is an agreement among 17 federal agencies, key among which are FEMA, the Nuclear Regulatory Commission (NRC), the Departments of Energy and Defense, and the Environmental Protection Agency (EPA).

Roots of the FRERP

From the time of its founding in 1970, EPA had responsibility for dealing with radiological emergencies, though an orchestrated federal response to such situations still lay many years in the future. In 1975, the General Services Administration (GSA) offered the first such plan, but the GSA, whose principal mission is the management of physical assets belonging to the government, was not the ideal agency to oversee emergency responses. Following the disaster at the Three Mile Island Nuclear Power Plant in 1979, President James E. Carter issued an executive order creating such an agency, FEMA.

In September 1980, Carter issued another executive order in which he called on FEMA to create a "national contingency plan" that would coordinate federal agencies' responsibilities and authorities in the event of a nuclear accident. FEMA in March 1982 established the Federal Radiological Preparedness Coordinating Committee, which consisted of representatives from federal agencies with responsibilities for responding to radiological emergencies. The purpose of the committee was to coordinate federal planning and preparedness activities, and to help state and local governments develop their own coordinated plans.

At the same time, FEMA directed the EPA to develop training for state and local officials in areas ranging from decision making to radiation dose assessment. The agency also tasked the Department of Energy (DOE) with putting in place systems for emergency radiation detection and measurement. FEMA also directed DOE to establish a federal radiological monitoring and assistance plan. Together with EPA, NRC, and other agencies, the DOE in the early 1980s developed the Federal Radiological Monitoring and Assessment Center (FRMAC) to implement the plan it developed. DOE maintains the FRMAC, but in the event of an emergency, EPA would assume control in the middle and latter phases of the crisis.

FRERP, other RERPs, and their evolution. The Federal Radiological Preparedness Coordinating Committee completed the FRERP in 1985, and in 1987 the EPA published its own RERP describing how it would support state and local agencies in the event of a radiological emergency. States have also developed their own RERPs. Following the accident at the Chernobyl Nuclear Power Plant in what was then the Soviet Union (now Ukraine) in April 1986, the Federal Radiological Preparedness Coordinating Committee revised the FRERP to include a response to international radiological incidents that could affect the United States.

The revised plan also incorporated responses to smaller situations, such as lost radiation sources or lost radioactive material. EPA was made the lead federal agency in both international and lost-course incidents. In 1989, EPA responded to such a situation, when it was discovered that abandoned materials at the Radium Chemical Company facility in New York City presented a radiological hazard to the neighborhood.

During the 1980s, participating organizations took part in two full-field exercises to prepare for a radiological emergency. In June 1995, President William J. Clinton signed Presidential Decision Directive (PDD) 39, which directed the response of federal agencies to terrorist attack. PDD 39 directed EPA to provide chemical and radiation-related technical support to the Federal Bureau of Investigation in the event of a terrorist incident. Additional directives in 1998 led to a revision of the EPA RERP in 2000.

FURTHER READING:

BOOKS:

Congel, F. J. *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants: Criteria for Protective Action Recommendations For Severe Accidents: Draft Report for Interim Use and Comment.* Washington, D.C.: U.S. Nuclear Regulatory Commission/Federal Emergency Management Agency, 1996.

PERIODICALS:

Muhlebach, Richard. "What's Your Disaster Plan?" *National Real Estate Investor* 44, no. 8 (August 2002): 64.

ELECTRONIC:

EPA's Radiation Protection Program: Emergency Response. Environmental Protection Agency. <http://www.epa.gov/radiation/rert/history.htm> (March 4, 2003).

Federal Radiological Emergency Response Plan. Florida Department of Community Affairs. <http://www.dca.state.fl.us/bpr/EMTOOLS/Nuclear/frerp.htm> (March 4, 2003).

SEE ALSO

Domestic Emergency Support Team, United States
Emergency Response Teams
Environmental Issues Impact on Security
EPA (Environmental Protection Agency)
FEMA (United States Federal Emergency Management Agency)
Nuclear Emergency Support Team, United States
Nuclear Regulatory Commission (NRC), United States

Reagan Administration (1981–1989), United States National Security Policy

CARYN E. NEUMANN

To Ronald Reagan, national security meant battling the Soviet Union for world supremacy. Much more conservative than his predecessors, Reagan argued that international instability of the world could be traced to Moscow and he insisted that the United States needed to use military force to protect its global interests. As a result of these assumptions, the Reagan administration promoted a massive buildup of both conventional and nuclear weapons to close the gap that it presumed had developed between Soviet and American forces.

Reagan had little foreign policy expertise. A popular actor who had served as governor of California, he won the presidency from Jimmy Carter in large part because he promised to engineer a return to the glory days of international respect for the U.S. To help achieve this goal, Reagan revamped the national security system. Secretary of State Alexander Haig served as the primary advisor on foreign affairs, while National Security Advisor (NSA) William Clark took responsibility for developing, coordinating, and monitoring national security policy.

Reagan made another significant change by terminating the policy of détente with the Soviet Union that had been pursued by his predecessors. He made this choice out of his expressed belief that the inherent evil of Soviet totalitarianism had created an "evil empire." He repeatedly stated the American resolve to fight communist aggression anywhere in the world. This determination would lead the U.S. to confront communism in Grenada, El Salvador, and Nicaragua, with the latter effort turning into the Iran-Contra scandal.

Reagan's actions were occasionally more moderate than his words and the administration appeared reluctant to be the first since World War II to fail to arrive at an agreement on arms with the Soviets. President Carter had negotiated the SALT II treaty but Reagan believed that it was fatally flawed. While agreeing to abide by the restrictions of the agreement as long as the Soviet Union did the same, Reagan refused to submit it to the Senate for ratification. In 1982, the administration announced the outlines of a replacement arms control treaty. To show displeasure with past agreements that merely reduced the growth of each side's arsenals instead of reducing the total numbers of weapons, the Reagan administration security team named the new arms control plan START (Strategic Arms Reduction Talks). This new arms policy was designed to bring about cuts in total American and Soviet missiles and warheads, but the two sides were unable to reach an agreement.

In 1983, Reagan escalated the nuclear arms race with the Soviet Union by authorizing the Defense Department to develop a Strategic Defense Initiative (SDI). Known to its advocates and critics as "Star Wars," SDI would involve the development of a complex anti-missile defense system employing laser and high-energy particle weapons to destroy enemy missiles in outer space before they reached their targets. By destroying weapons rather than people, SDI would free defense strategy from the concept of mutually assured destruction that had long governed Soviet and American attitudes toward war. Although the system was never built and many scientists doubted that it could ever be constructed in the form proposed, the Soviets felt obligated to keep pace by launching their own SDI-type development program.

By the end of Reagan's presidency, his anti-Soviet rhetoric had cooled. Under Mikhail Gorbachev, the Soviets pursued renewed détente and the Reagan administration responded positively. In 1987, the U.S. and U.S.S.R. signed a treaty to eliminate intermediate range (300 to 3,000 miles) nuclear forces (INF). The agreement marked the first time that the two nations had agreed to destroy an entire class of weapons systems.

Reagan entered the White House with a campaign promise to refurbish American defense capabilities and to regain military superiority over the Soviet Union. He exited the Oval Office after completing a treaty that served as the first step toward the eventual end of the arms race. By redirecting the thrust of national security policy, the Reagan administration is widely credited with winning the Cold War.

In the shadow of an American M-60 tank, two U.S. soldiers stand guard over three Grenadian prisoners. President Ronald Reagan ordered the invasion of Grenada in 1983 in order to oust its Marxist government. AP/WIDE WORLD PHOTOS.

FURTHER READING:

BOOKS:

Boll, Michael M. *National Security Planning Roosevelt Through Reagan.* Lexington: University Press of Kentucky, 1988.

Thomson, Kenneth W., ed. *The Reagan Presidency.* Lanham, MD: University Press of America, 1997.

ELECTRONIC:

White House. "History of the National Security Council, 1947–1997." <http://www.whitehouse.gov/nsc/history.html> (April 25, 2003).

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union
Iran-Contra Affair
National Security Strategy, United States
START I Treaty

Real IRA (RIRA)

The Real Irish Republican Army (Real IRA, or RIRA), also known as the the True IRA, formed in early 1998 as a clandestine armed wing of the 32-County Sovereignty Movement, a "political pressure group" dedicated to removing British forces from Northern Ireland and unifying Ireland. The 32-County Sovereignty Movement opposed Sinn Fein's adoption in September, 1997, of the Mitchell principles of democracy and nonviolence and opposed

the amendment in December 1999 of Articles 2 and 3 of the Irish Constitution, which laid claim to Northern Ireland. Michael "Mickey" McKevitt, who left the IRA to protest its cease-fire, leads the group; Bernadette Sands-McKevitt, his wife, is a founder-member of the 32-County Sovereignty Movement, the political wing of the RIRA.

Organization activities. The Real IRA has claimed to have committed or is believed to be responsible for a number of bombings, assassinations, and robberies. Many Real IRA members are former Irish Republican Army (IRA) members who left that organization following the IRA cease-fire and who bring to RIRA a wealth of experience in terrorist tactics and bomb construction. RIRA targets include British military and police in Northern Ireland and Northern Ireland Protestant communities. RIRA is linked to and understood to be responsible for the car bomb attack in Omagh, Northern Ireland, on August 15, 1998, that killed 29 and injured 220 persons. The group began to observe a cease-fire following Omagh but in 2000 and 2001 resumed attacks in Northern Ireland and on the UK mainland against targets such as MI6 headquarters and the BBC.

RIRA's size is estimated at 100 to 200 activists plus possible limited support from IRA hardliners dissatisfied with the IRA cease-fire and other republican sympathizers. British and Irish authorities arrested at least 40 members in the spring and summer of 2001, including leader McKevitt, who is currently in prison in the Irish Republic awaiting trial for being a member of a terrorist organization and directing terrorist attacks.

Suspected of receiving funds from sympathizers in the United States and of attempting to buy weapons from U.S. gun dealers, RIRA also is reported to have purchased sophisticated weapons from the Balkans. Three Irish nationals associated with RIRA were extradited from Slovenia to the UK and are awaiting trial on weapons procurement charges.

As of April 2003, the U.S. Department of State no longer listed the IRA as a foreign terrorist organization, but did list the Real IRA. The RIRA operates in Northern Ireland, Irish Republic, and Great Britain.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Reconnaissance

Reconnaissance is a term for efforts to gain information about an enemy, usually conducted before, or in service to, a larger operation. The French word entered the English language in 1810—not coincidentally, at a time when British and other armies were at war with Napoleon's French forces. Reconnaissance is an important component of military and intelligence activities, as well as civilian undertakings designed to protect the public safety from hazards both natural and manmade.

In the military or espionage environment, reconnaissance can take the form of activities by scouts or other specialists. The use of what would now be called "human intelligence" in a reconnaissance capacity dates back to ancient times, when, according to the Christian Old Testament, 12 spies went into the land of Canaan to scout out the territory. Today, reconnaissance is the work of special units practicing a specialized craft.

Reconnaissance aircraft range from the U-2 and SR-71 Blackbird to the E-2C Hawkeye and P-3 Orion. Additionally, the skies bristle with reconnaissance satellites operated by the U.S. military, the National Security Agency, and military or intelligence services of other nations. Even some seagoing craft, most notably submarines, can serve a reconnaissance function.

The major reconnaissance components of the U.S. intelligence community are the National Reconnaissance Organization and the National Imagery and Mapping Agency. In the civilian realm are meteorological services such as the National Oceanic and Atmospheric Administration, which makes extensive use of reconnaissance technology to map and forecast weather patterns. Additionally, the Department of Energy, Environmental Protection Agency, and other organizations conduct reconnaissance for radiological hazards and other forms of danger.

FURTHER READING:

BOOKS:

Burrows, William E. *By Any Means Necessary: America's Secret Air War in the Cold War.* New York: Farrar, Straus and Giroux, 2001.

Day, Dwayne A., and John M. Logsdon. *Eye in the Sky: The Story of the Corona Spy Satellites.* Washington, D.C.: Smithsonian Institution Press, 1998.

Gann, Ernest. *The Black Watch: The Men Who Fly America's Secret Spy Planes.* New York: Random House, 1989.

Osborn, Shane, and Malcolm McConnell. *Born to Fly: The Untold Story of the Downed American Reconnaissance Plane.* New York: Broadway Books, 2001.

ELECTRONIC:

National Imagery and Mapping Agency. <http://www.nima.mil/> (April 1, 2003).

National Reconnaissance Office. <http://www.nro.gov/> (April 1, 2003).

SEE ALSO

Balloon Reconnaissance, History
E-2C
NIMA (National Imagery and Mapping Agency)
NRO (National Reconnaissance Office)
P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft
Photographic Interpretation Center (NPIC), United States National
Photography, High-Altitude
Satellites, Spy

Red Brigades.

SEE *Anti-Imperialist Territorial Nuclei (NTA).*

Red Code

Red was a Japanese naval code created during World War I and used until the outbreak of World War II. The Red code used the additive encryption method. The code assigned words and syllables numerical values. Before transmissions, these numbers were encrypted a second time using an additive codebook. The book contained a series of numbers that were added to the original numerical message in sequence. Each message contained a key that told the receiver where to begin the additive sequence in the book to decode the message. Cryptologists named the code Red after the color of the folder in which deciphered codes were bound.

In 1923, a United States Navy intelligence officer located a copy of the 1918 Imperial Japanese Navy secret operating code in the luggage of a visiting Japanese attaché. The codebook was clandestinely photographed and a special cryptology unit, known as the Research Desk, was created to begin the task of monitoring and deciphering intercepted messages. At the time, U.S. Navel Intelligence monitored only ship-to-ship communications and some radio transmissions in Asia and the Pacific. The Research Desk team established intercept stations throughout the Pacific and increased monitoring of Japanese diplomatic and military transmissions.

Cryptologists worked for five years to fully translate and break Red, the additive cipher that the 1918 codebook contained. Intercepts continued to use the aging code, facilitating the work of U.S. code breakers. In 1926, Lieutenant Joseph J. Rochefort accepted the directorship of the Research Desk. Rochefort was a skilled code breaker, but also fluent in the Japanese language and undertook much of the translation work for Red himself. Repeated messages and phrases that appeared in several transmissions helped code breakers recognize various additive decipherments. Three years after the analysis of Red began, cryptologist Agnes Meyer Driscoll cracked the code's additive encryption key. With the additive key, and the photographs of the original code book, any Red code message could be deciphered.

The Japanese replaced Red with a more sophisticated code on December 1, 1930. However, the new code, called Blue, contained numeric patterns that so closely resembled Red that Driscoll and her team were able to decipher and translate Blue in only two years.

■ FURTHER READING:

BOOKS:

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II.* New York: Touchstone Books, 2002.

Matthews, Tony. *Shadows Dancing: Japanese Espionage Against the West.* New York: St. Martin's Press, 1993.

SEE ALSO

Purple Machine
World War II, United States Breaking of Japanese Naval Codes

Red Hand Defenders (RHD)

Red Hand Defenders (RHD) is an extremist terrorist group formed in 1998 and composed largely of Protestant hardliners from loyalist groups observing a cease-fire. RHD seeks to prevent a political settlement with Irish nationalists by attacking Catholic civilian interests in Northern Ireland. In July, 2001, the group issued a statement saying it considered all nationalists "legitimate targets." RHD is a cover name often used by elements of the banned Ulster Defense Association and the Loyalist Volunteer Force. In recent years, the group has carried out numerous pipe bombings and arson attacks against "soft" civilian targets such as homes, churches, and private businesses, including a bombing outside a Catholic girls school in North Belfast. RHD claimed responsibility for the car-bombing murder in March, 1999, of Rosemary Nelson, a prominent Catholic nationalist lawyer and human rights

campaigner in Northern Ireland, and for the murder of a Catholic journalist in September, 2001.

The RHD may have up to 20 members acting in Northern Ireland, some of whom have considerable experience in terrorist tactics and bombmaking.

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Red Orchestra

The Red Orchestra was the name given to a network of communist, Soviet-affiliated spies during World War II. The group provided intelligence to the Soviet government, but also functioned as a resistance organization against the Nazis. During its three years in operation, the Red Orchestra smuggled key German secrets and documents to Allied forces, and rescued several political prisoners, mostly communist dissidents.

Leopold Trepper, a Polish-born Jew and communist activist, joined the Soviet Red Army Intelligence Service in the mid-1930s. He was later assigned to the Peoples Commissariat for Internal Affairs (NKVD), a fledgling Soviet secret police and espionage agency. Before World War II began in Europe, Trepper established a network of communist sympathizers and leftist political activists. When the war began in 1939, Trepper turned his network into a spy ring, bent on gathering Nazi secrets and other intelligence useful to the Soviet army.

Trepper's network, the Red Orchestra, soon had operating divisions, or rings, in Nazi occupied France, Belgium, Holland, and neutral Switzerland. Each ring had varying successes. The French unit provided information to Resistance fighters and infiltrated several Nazi offices in Paris, stealing documents and radio equipment. Red Orchestra agents infiltrated the German military intelligence Abwehr headquarters in Paris and successfully tapped its phones. This permitted agents to intercept intelligence information transmitted directly from Berlin.

The greatest espionage achievement of the organization, however, was that of the Swiss ring, nicknamed Lucy. The Red Orchestra unit received leaked information and a document relating to the Nazi plan to invade the Soviet Union. These documents, which included the proposed date for the launch of the offensive, were turned over to the Soviet army and government, but were wholly ignored.

Trepper's network began to crumble in 1942, when several Red Orchestra agents were arrested in Belgium. Later that year, the Gestapo tracked down Trepper himself and arrested him in Paris. The Gestapo managed to find and eliminate many Red Orchestra agents. Some rings continued to operate throughout the war, but on a smaller scale. Trepper escaped his Nazi captors and tried to rebuild his group, but by 1944 the Red Orchestra network had been largely dissolved.

■ FURTHER READING:

BOOKS:

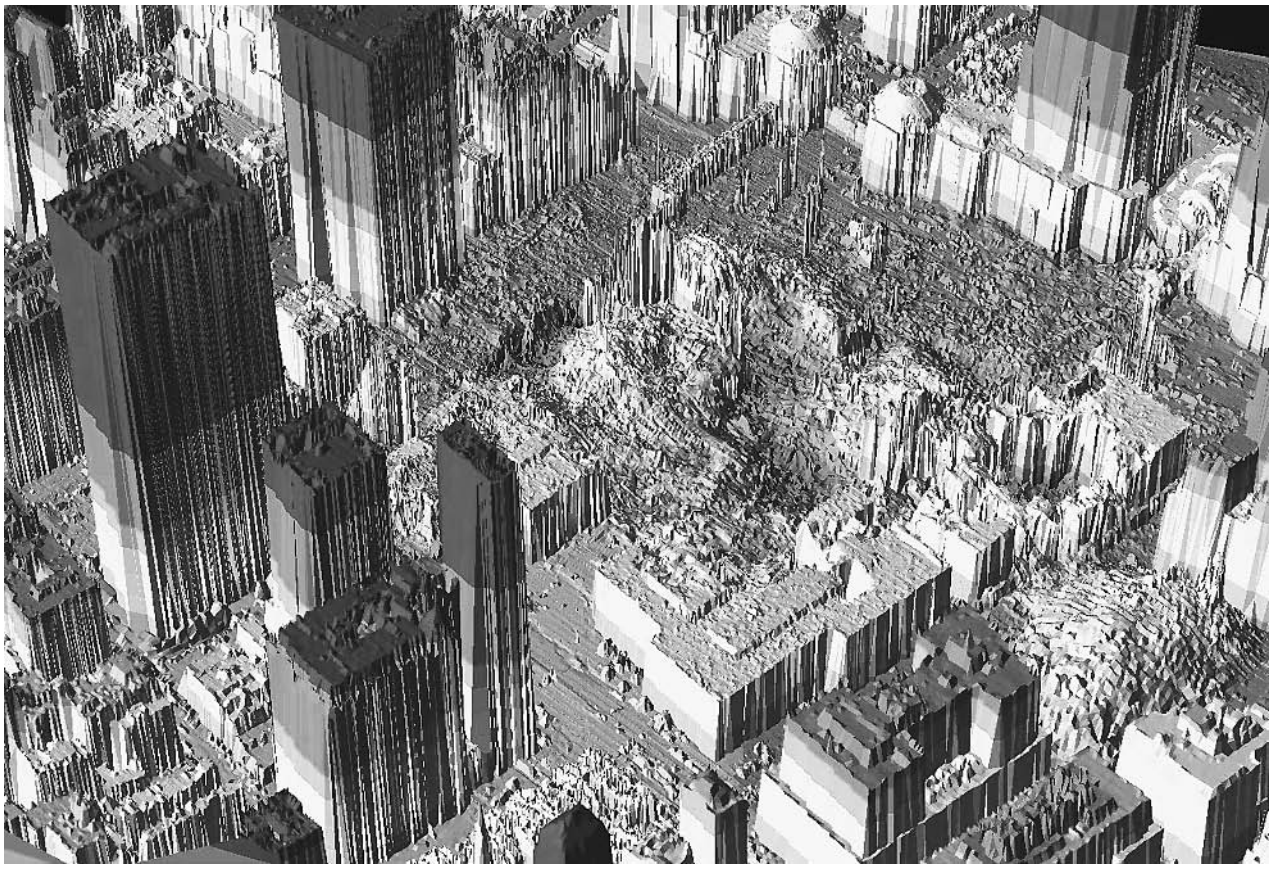
Tarrant, V. E. *The Red Orchestra, the Soviet Spy Network Inside Nazi Europe.* New York: Bantam, 1996.

Remote Sensing

■ WILLIAM C. HANEBERG

Remote sensing is the acquisition of information about an object or phenomenon by a device located a considerable distance from the object or phenomenon. The term was coined in the mid-1950s by an Office of Naval Research scientist to distinguish the information obtained from the first generation of meteorological satellites from that which had been traditionally obtained by airplane-based aerial photography. In practice, however, information obtained from high-flying reconnaissance aircraft such as the U-2 and SR-71 can also be considered to be a product of remote sensing.

In addition to providing panchromatic (black and white) and multispectral color images that resemble photographs, some modern remote sensing satellites contain hyperspectral sensors that record information using dozens or hundreds of reflected electromagnetic energy wavelength bands that extend beyond the range of human vision. The simplest kind of multispectral image consists of red, blue, and green bands added together to form a color composite image. Image processing software can be used, particularly with hyperspectral data, to identify the chemical composition of rocks, vegetation type, soil or



This LIDAR photo shows elevations at the World Trade Center site in New York on September 19, 2001. LIDAR is short for Light Detection and Ranging, a remote sensing technique.

water pollution, and other attributes that can be characterized in terms of spectral reflectance. Paired images can also be used to stereoscopically construct digital elevation models (DEMs), which can subsequently be transformed into topographic maps or three dimensional terrain models from space.

Other satellites contain active sensors that generate their own electromagnetic signals and record the reflections rather than passively recording reflected natural radiation. Synthetic aperture radar (SAR), in particular, is a useful tool because it can penetrate clouds and be used at night. The length of a radar antenna is known as its aperture and, in general, the resolution of a radar image is proportional to antenna length. The term synthetic aperture refers to a technique in which the constant movement of a satellite is combined with periodic radar pulses and computer processing to achieve the same effect as would be obtained by using a very large antenna. Pairs of SAR images can be combined to produce interferometric (InSAR) images that portray millimeter to centimeter scale changes in the elevation of Earth's surface. InSAR is becoming an increasingly important tool for monitoring tectonic movements of Earth's crust, subsidence associated with heavy groundwater pumping, and other geologic processes. It can also be used to construct digital elevation models. Another active source remote sensing technique is light detection and ranging (LIDAR), which is similar to radar but uses a laser instead of radio waves to produce extremely detailed topographic maps and images.

It is generally understood that remote sensing satellites must have a resolution of 5 meters (m) or less to be useful for intelligence work. The Landsat 1 satellite, launched by the United States in 1972 and from which imagery was freely available, had a resolution of 80 m. Landsat 7, launched in 1999 and still in service, has resolutions of 15 m for panchromatic images, 30 m for its six multispectral bands, and 60 m for its thermal band. The French SPOT 5 satellite offers commercially available images ranging in resolution from 5 m for panchromatic to 20 m for infrared. Publicly available images with these coarse resolutions are useful for such tasks as delineating large-scale geologic features, evaluating inaccessible or denied terrain, examining land use patterns, and inferring levels of crop stress, but not for detailed intelligence work. In recent years, however, commercial remote sensing satellites have been able to obtain high-resolution images that are of intelligence quality. The commercial QuickBird satellite launched from Vandenberg Air Force Base in late

2001, for example, provides commercially available imagery with 61 cm panchromatic and 2.44 m multispectral resolution. The commercial IKONOS satellite, launched in 1999, can produce 1 m resolution color images.

Even the best publicly available imagery does not approach the resolution provided by classified intelligence satellites. The earliest KeyHole intelligence satellites (KH1 series), the first of which was launched by the United States in 1960, had a resolution of 2 m. Photographic film from KeyHole satellites was recovered using film drops until 1972, when digital imaging and transmission were instituted. The KH12 series is estimated to have a resolution of approximately 2 cm, although no images with this resolution have been released. Intelligence-quality images with sub-meter resolution can be used to assess details of troop or materiel movement, the progress of construction projects, and war damage in denied or otherwise inaccessible areas. Perhaps the most widely known application of remotely sensed images for intelligence work was the use of satellite and U-2 airplane photographs to detect the presence of Russian missiles in Cuba, which led to the 1962 Cuban missile crisis.

FURTHER READING:

BOOKS:

Campbell, James B. *Introduction to Remote Sensing, 3rd ed.* New York: Guilford Press, 2002.

ELECTRONIC:

Hardin, R. Winn. "Remote Sensing Satellite Market Pits Industry Against U.S. Policy." OE Reports. May 1999. <http://www.spie.org/app/publications/magazines/oerarchive/may/may99/cover1.html> (November 14, 2002).

Short, Nicholas M., Sr. "The Remote Sensing Tutorial." NASA. October 22, 2002. <http://rst.gsfc.nasa.gov/> (November 14, 2002).

Skorve, Johnny E. "Using Satellite Imagery to Map Military Bases of the Former Soviet Union." Earth Observation Magazine. April 2002. <http://www.eomonline.com/Common/currentissues/Apr02/skorve.htm> (November 14, 2002).

International Society for Photogrammetry and Remote Sensing, Department of Geomatic Engineering, University College London, Gower Street, London WC1E 6BT, United Kingdom. 44 207679 7226. <http://www.isprs.org/.> (November 14, 2002).

SEE ALSO

Bomb Damage, Forensic Assessment
Cameras
Cuban Missile Crisis
Electromagnetic Spectrum
Electro-optical Intelligence
Geospatial Imagery
LIDAR (Light Detection and Ranging)
Photographic Resolution
Photography, High-Altitude
RADAR, Synthetic Aperture
U-2 Spy Plane
Unmanned Aerial Vehicles (UAVs)

Remote Sentinels.

SEE *Biological Input/Output Systems (BIOS).*

Retina and Iris Scans

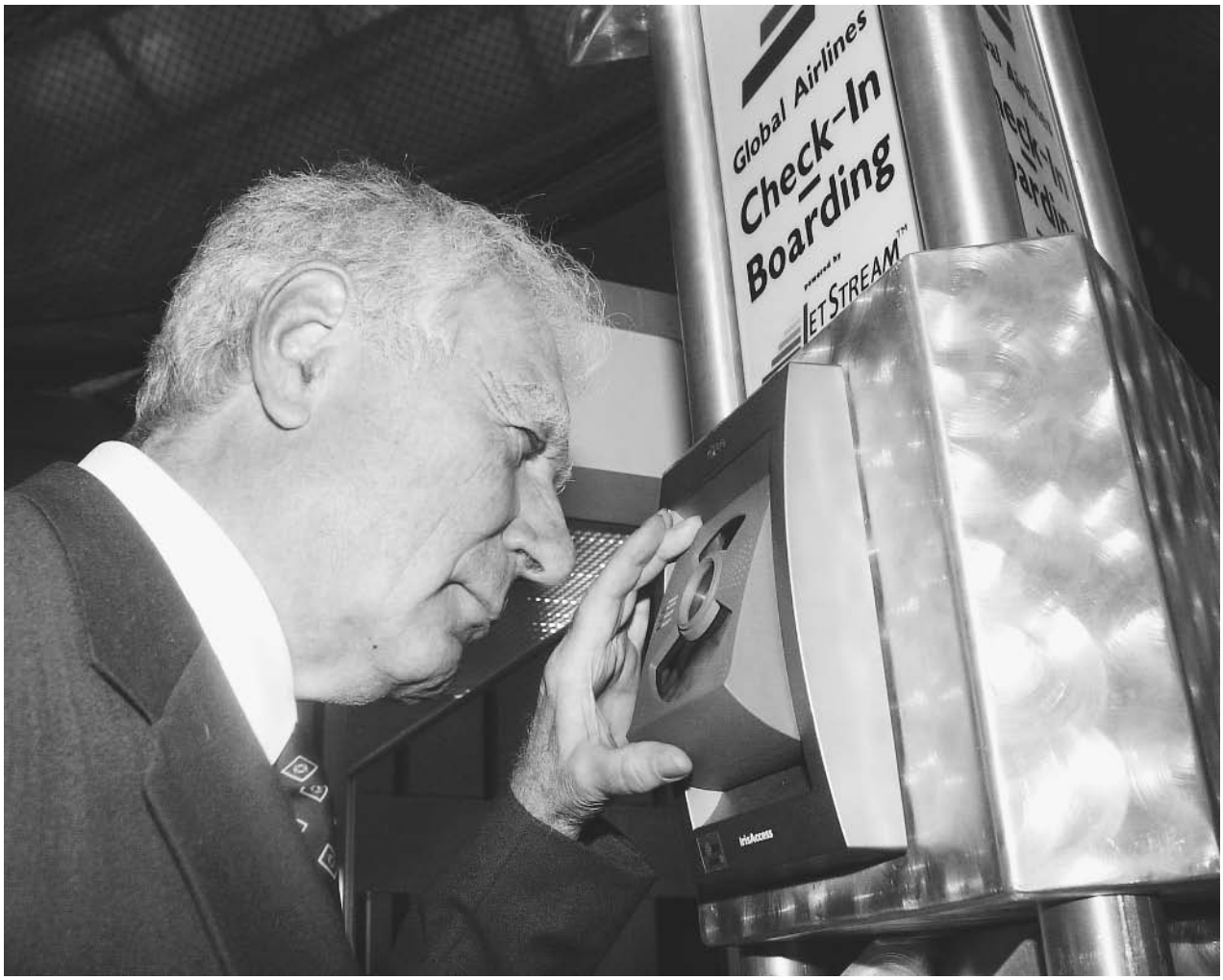
AGNIESZKA LICHANSKA

The retina is the neural part of the eye responsible for vision and the pattern of blood vessels serving the retina is as unique as a fingerprint.

The technology that scans the retina is known as retinal scanning. The true target for the scan is the capillary pattern in the retina. The process relies on generating images of the retina using a low-intensity light source. In the 1930s retinal capillary patterns were suggested to be unique, but the technology used to exploit this information was developed much later. Although military and high-security use of photographic retinal scans began decades earlier, by 1985, retinal scan technology became available for computerized biometric identification and commercial security use.

Retinal scans are just one of the biometric methods using the eye for personal identification. Two years after the first retinal scanner was developed in 1987, Leonard Flom and Aram Safir patented the use of the iris as a personal identifier. However, it was not until 1994 when John Daugman developed the technology for iris scanning that is became useful, and since then iris scanning has begun to challenge the retinal scans. Currently a number of companies claiming that they perform retinal scanning, in reality are performing iris scans.

Retina scanning procedures. Retinal scans are based on the presence of the fine network of capillaries supplying the retina with oxygen and nutrients. These vessels absorb light and can be easily visualized with proper illumination. Retinal scans require close contact of user and scanner, a perfect alignment of the eye with a scanner, and no movement of the eye. The examiner is required to keep the subject's eye within half an inch of the instrument. The subject must focus on a pinpoint of little green light (to properly align the eye) and avoid blinking. A low-intensity coherent light is then transmitted through the eye and the reflected image of the retinal capillary pattern is recorded by the computer.



An executive demonstrates a retinal scanner used for identification at the International Air Transport Association security symposium in Atlanta in 2001. AP/WIDE WORLD PHOTOS.

Although retinal patterns are generally thought to be constant during a person's life, they can change in case of diabetes, glaucoma, retinal degenerative disorders or cataracts. Therefore, although retinal scans are nearly 100% accurate they cannot be used as a universal security measure without making allowances for normal changes.

An initial scan (enrollment) takes a minimum of five scans and lasts approximately 45 seconds; subsequent authentication scans are faster and take only 10–15 seconds. An acquired image containing 320–400 reference points is converted to a map of the retina and used to identify a match from the templates encoded in the scanner's software. Retinal images captured are extremely small, only 35 bytes in size.

Retinal scans versus iris scans. Retinal scans are considered to be too intrusive for a general security use and the prolonged exposure to light emitted by the scanners might be harmful to the eye. As a result a strong competition to the retinal scans was launched by iris scanning technology. The number of companies offering iris scanning are increasing. The main reason is the fact that the iris is also unique and offers high confidence in identification. There is only a chance of one in 10^{78} that two irises will be identical.

Iris scans use the characteristics more similar to fingerprints than to the retinal vein pattern. The colored part of the eye appears to be as unique as fingerprints and retina. Scanning technology takes advantage of crypts, furrows, ridges, striatations, ligaments, and collarette. While 240 points are recorded, the image size is 512 bytes, over ten times larger than a retinal scan. The main advantage of the iris scans is the ability to perform them from a distance of up to three feet and short time of scan of only 20 seconds initially, with subsequent identification requiring only two seconds. Glasses and contact lenses do not interfere with the scanning process and identification.

Scanners. The technology for retinal scans has changed in recent years. The initial large devices are now being replaced by smaller and more accurate instruments. The first commercial retinal scanner was developed by EyeDentify in 1984 with the launch of the Eyedentification 7.5 personal identification unit. One of the most recent developments in the area is a small mobile and easy to use retinal scanner developed by Retinal Technologies from Boston. Although it was initially developed for diagnostic purposes it will be available as a security tool as well.

Fooling the retinal scanner is very difficult, as they require intact retinas to complete a scan. Following death, the retina degrades very quickly and thus cannot be used in most cases for accurate post-mortem identification. Although often a popular movie special effect, using a retina detached from a cadaver would fail to pass notice by modern scanning equipment. Likewise, surgical alteration of the retinal pattern would be not only a dangerous and extremely expensive process, but the changes introduced would be readily detected by modern scanning equipment.

In contrast to the retinal scanners, iris scanners are of two main types: active and passive. The active system works from 3 to 14 inches and also requires the user to move forward and backwards so the camera is adjusted properly. In contrast the passive system can work over longer distances one to three feet. The main technology developer is Iridian Technologies, which holds the patents to the concepts and technologies involved.

Security uses of retinal and iris scans. Biometric techniques are used in identification and authentication. The features used for the two processes can overlap or can be different. Authentication requires high accuracy to ensure restricted access. Retinal and iris scans offer high accuracy, and the primary users of retinal scans are military and government facilities, such as CIA, FBI, and NASA. Scans are used to control access to high security areas. The technology is currently spreading beyond these institutions and is being used by Cook County Prison in Illinois (to ensure the identity of the prisoners) as well as General Dynamics (a defense contractor).

Some of the Japanese banks use retinal scans in ATM machines to prevent unauthorized use of the system. Trials in the USA with biometric ATM security are using iris recognition systems instead. However, in Illinois retinal scans in conjunction with fingerprinting are used to prevent welfare fraud.

Acceptance is growing for the iris recognition systems and they are now used by government agencies, commercial companies, and in the public sector. Among the government users are the U.S. Congress and the Departments of Defense, State and Treasury. Commercial companies that protect themselves by using iris recognition include Bank United, GTE, Hewlett Packard, Lockheed Martin, and British Telecom. Other places with restricted access areas, including airports, have acquired scanning technologies in the wake of the September 11, 2001, terrorist attacks upon the United States. Scanning technology systems were recently installed at Charlotte (North Carolina), Amsterdam (Netherlands) and Frankfurt (Germany) mainly for security purposes to check the employees and provide controlled access to the secure areas of the airports. Studies are underway to test if scanning technologies can be used to facilitate rapid check in and to streamline border crossing. The Schipol Airport in Amsterdam is one of the most recent airports to test the iris recognition system. The details of an individual's iris are stored on a special card and a subsequent check-in is performed by a simple iris scan to confirm identity. Eight of the largest Canadian airports (Toronto, Vancouver, Ottawa, Montreal, Halifax, Winnipeg, Calgary and Edmonton) plan to install similar systems by the end of 2003.

Scanning is also becoming part of security measures for sports and entertainment venues. For example, organizers at the 2002 Sydney Olympics used an iris scanning system termed EyeTicket. Use of retinal scans outside the high security areas is, in many areas, being replaced by iris scanning, which is easier to perform, is less intrusive for the user, and provides adequately accurate identification.

■ FURTHER READING:

BOOKS:

Ashbourn, Julian. *Advanced Identity verification. The complete guide.* London: Springer Verlag, 2000.

Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biometrics: Identity Verification in a Networked World.* New York: Wiley and Sons, 2002.

PERIODICALS:

French, M. "Retinal eyes biometric security. Company reveals its scanning technology." *Mass High Tech, The Journal of New England Technology,* 32 (2001).

ELECTRONIC:

DORO Inc. <http://www.dorosecurity.com/index2.html>(14 December 2002).

Court Technology Laboratory. "Biometrics and the Courts. Individual biometrics." <http://ctl.ncsc.dni.us/> (14 December 2002).

Find Biometrics. The complete biometrics resource guide for identification and verification. <http://www.findbiometrics.com/index.html> (14 December 2002).

Global Analytic Information Technology Services. "Retinal scanning." <http://www.gaits.com/biometrics_retinal.asp> (14 December 2002).

IridianTech. <http://www.iridiantech.com.> (14 December, 2002).

SEE ALSO

Biological and Biomimetic Systems
Biomedical Technologies

Bio-Optic Synthetic Systems (BOSS)
Fingerprint Analysis

Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Revolutionary Armed Forces of Colombia (FARC)

The Revolutionary Armed Forces of Colombia (FARC) was established in 1964 as the military wing of the Colombian Communist Party. FARC is Colombia's oldest, largest, most capable, and best-equipped Marxist insurgency. FARC is governed by a secretariat, led by Manuel Marulanda (a.k.a. "Tirofijo") and six others, including senior military commander Jorge Briceno (a.k.a. "Mono Jojoy"). FARC is organized along military lines and includes several urban fronts. In 2001, the group continued a slow-moving peace negotiation process with the Pastrana administration that has gained the group several concessions, including a demilitarized zone used as a venue for negotiations.

Organization activities. FARC is responsible for bombings, murder, kidnapping, extortion, hijacking, as well as guerrilla and conventional military action against Colombian political, military, and economic targets. In March, 1999, FARC executed three U.S. Indian rights activists on Venezuelan territory after kidnapping them in Colombia. Foreign citizens often are targets of FARC kidnappings for ransom. The group has well-documented ties to narcotics traffickers, principally through the provision of armed protection.

FARC has approximately 9,000 to 12,000 armed combatants and an unknown number of supporters, mostly in rural areas. FARC operates in Colombia with some activities in Venezuela, Panama, and Ecuador, while Cuba provides FARC some medical care and political consultation.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations

Revolutionary Nuclei

Revolutionary Nuclei (RN) (also known as Revolutionary Cells) emerged from a broad range of antiestablishment and anti-U.S./NATO/EU leftist groups active in Greece between 1995 and 1998. The group is believed to be the successor to or offshoot of Greece's most prolific terrorist group, Revolutionary People's Struggle (ELA), which, as of mid-2002, had not claimed an attack since January 1995. Indeed, RN appeared to fill the void left by ELA, particularly as lesser groups faded from the scene. RN's few communiqués show strong similarities in rhetoric, tone, and theme to ELA proclamations. RN claimed an attack in November, 2000.

Organization activities. Beginning operations in January 1995, RN has claimed responsibility for some two dozen arson attacks and bombings against a range of U.S., Greek, and other European targets in Greece. In its most infamous and lethal attack to date, the group claimed responsibility for a bomb it detonated at the Intercontinental Hotel in April 1999 that resulted in the death of a Greek woman and injured a Greek man. RN's *modus operandi* includes warning calls about impending attacks, attacks targeting property rather than individuals; use of rudimentary timing devices; and strikes during the late evening to early morning hours. RN last attacked U.S. interests in Greece in November 2000 with two separate bombings against the Athens offices of Citigroup and the studio of a Greek-American sculptor. The group also detonated an explosive device outside the Athens offices of Texaco in December 1999. Greek targets have included court and other government office buildings, private vehicles, and the offices of Greek firms involved in NATO-related defense contracts in Greece. Similarly, the group has attacked European interests in Athens, including Barclays Bank in December 1998 and November 2000.

RN membership is believed to be small, probably drawing from the Greek militant leftist or anarchist milieu. The RN's primary area of operation is in the Athens metropolitan area, and it is assumed to be a self-sustaining organization.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record

Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Revolutionary Organization 17 November (17 November)

The Revolutionary Organization 17 November (a.k.a. 17 November) is a radical leftist group established in 1975 and named for the student uprising in Greece in November, 1973, in protest of the military regime. Seventeen November has an agenda that is anti-Greek establishment, anti-U.S., anti-Turkey, anti-NATO, committed to the ouster of U.S. bases, removal of Turkish military presence from Cyprus, and the severing of Greece's ties to NATO and the European Union (EU).

Organization activities. Seventeen November's initial attacks were assassinations of senior U.S. officials and Greek public figures. The group added bombings in the 1980s and, since 1990, has expanded targets to include EU facilities and foreign firms investing in Greece. Seventeen November adherents are known to use improvised rocket attacks. In June, 2000, 17 November claimed responsibility for the murder of British Defense Attaché Stephen Saunders.

Operating in or near Athens, Greece, the exact size of 17 November is unknown, but membership is presumed to be limited to a small cadre.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Revolutionary People's Liberation Party/Front (DHKP/C)

The Revolutionary People's Liberation Party/Front (DHKP/C) was originally formed in 1978 as Devrimci Sol, or Dev Sol, a splinter faction of the Turkish People's Liberation Party/Front. Renamed in 1994 after factional infighting, it espouses a Marxist ideology and is virulently anti-U.S. and anti-NATO. The organization finances its activities chiefly through armed robberies and extortion. It also operates as, or is known as Devrimci Sol, Revolutionary Left, and Dev Sol.

Organization activities. Since the late 1980s, the DHKP/C has concentrated attacks against current and retired Turkish security and military officials. The group began a new campaign against foreign interests in 1990. DHKP/C adherents assassinated two U.S. military contractors and wounded a U.S. Air Force officer to protest the Gulf War. The group launched rockets at the U.S. Consulate in Istanbul in 1992. In early 1996, the group assassinated a prominent Turkish businessman and others, its first significant terrorist acts as DHKP/C. Turkish authorities thwarted DHKP/C attempts in June, 1999, to fire light antitank weapons at the U.S. Consulate. DHKP/C conducted its first suicide bombings, targeting Turkish police, in January and September 2001. A series of safehouse raids and arrests by Turkish police over the last few years have weakened the group significantly.

The exact membership in the Revolutionary People's Liberation Party/Front is unknown. DHKP/C conducts attacks in Turkey, primarily in Istanbul, and raises funds in Western Europe.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001. Annual Report: On the Record

Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Revolutionary Proletarian Initiative Nuclei (NIPR)

Revolutionary Proletarian Initiative Nuclei (NIPR) is a clandestine leftist extremist group that appeared in Rome in 2000. NIPR adopted the logo of the Red Brigades of the 1970s and 1980s—an encircled five-point star—for their declarations. NIPR opposes Italy's foreign and labor policies and claimed responsibility for the bomb attacks in April, 2001, on a building housing a U.S.-Italian-relations association and on an international affairs institute in Rome's historic center. NIPR claimed to have carried out a May, 2000, explosion in Rome at an oversight committee facility for implementation of the law on strikes in public services as well as an explosion in February, 2002, on the Via Palermo adjacent to the Interior Ministry in Rome.

Comprising about a dozen members, NIPR operates mainly in Rome, Milan, Lazio, and Tuscany.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001." Annual Report: On the Record Briefing. May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Revolutionary United Front (RUF)

Revolutionary United Front (RUF) is a loosely organized guerrilla force seeking to retain control of the lucrative diamond-producing regions of Sierra Leone. The group funds itself largely through the extraction and sale of diamonds obtained in areas of Sierra Leone that it controls. During 2001, reports of serious abuses by the RUF declined significantly. The resumption of the government's Disarmament, Demobilization, and Reintegration program in May was largely responsible. From 1991 to 2000, the group used guerrilla, criminal, and terror tactics, such as murder, torture, and mutilation, to fight the government, intimidate civilians, and keep U.N. peacekeeping units in check. In 2000, they held hundreds of U.N. peacekeepers hostage until their release was negotiated, in part, by the RUF's chief sponsor, Liberian president Charles Taylor. The group also has been accused of attacks in Guinea at the behest of President Taylor.

RUF's strength is estimated at several thousand supporters and sympathizers who operate in Sierra Leone, Liberia, and Guinea. A UN experts panel report on Sierra Leone asserted that President Charles Taylor of Liberia provided support and leadership to the RUF. The UN has identified Libya, Gambia, and Burkina Faso as conduits for weapons and other materiel for the RUF.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins

Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Revolutionary War, Espionage and Intelligence

ADRIENNE WILMOTH LERNER

The American Revolution officially began with the signing of the Declaration of Independence on July 4, 1776. However, the conflict between Britain and the American colonies escalated to full-scale war from several orchestrated acts of subversion against British authority. High taxation, shipping restrictions, controls on employment and land ownership, as well as lack of representation in British government prompted resistance to British laws by American colonial citizens. The first shots of the Revolution are said to be those that occurred during the Boston Massacre, the British armed retribution for acts of sabotage against British interests, including the events of the Boston Tea Party. The conflict ended with the Treaty of Paris in 1783, granting international recognition for the newly independent United States. The Revolution marked the beginning of a new era in international politics, shifting the world balance of power and military might over the next 230 years.

Formation of the United States Intelligence Community

At the outbreak of war, the fledgling American government had few resources, and was still divided by the competing interests of rival colonies. Many leaders were suspicious of establishing permanent, national militaries. The American colonies had to recruit volunteers, train, and arm soldiers, a daunting task for the new nation. Colonial militias aided in training soldiers, and at the outbreak of the war, American military command decided to use their more limited forces in guerilla attacks against the stronger, more formalized British army.

In addition to troop strength and weaponry, the British had the significant advantage of having a developed strategic intelligence force within its military corps. The British established a network of Loyalist spies and informants, many of whom were able to infiltrate and report on American military formation, tactics, battle plans, and defensive positions. This espionage gave Britain a decided upper hand in the early months of the conflict, with devastating effect on the American armies.

A statue of Nathan Hale, a revolutionary soldier who was captured and hung by the British for espionage, in front of the Tribune Tower, in Chicago, Illinois. ©SANDY FELSENTHAL/CORBIS.

Before the outbreak of the Revolution, the American colonial government, the Continental Congress, created the Committee of Correspondence in 1775. The purpose of the committee was to establish foreign alliances and gain the aid of foreign intelligence resources. The original intent of the committee was to facilitate the sharing of information about British colonial policy, but at the start of the Revolution, the Committee seized and combed mail for vital intelligence information. The organization was renamed the Committee of Secret Correspondence, and then the Committee of Foreign Affairs, and employed trusted Patriot sympathizers in Britain to feed American leaders intelligence information. After establishing protocol for obtaining information, the committee established a network of couriers to disperse information to battlefield commanders and key government officials. The committee also sought the aid of French forces in the war effort.

The Second Continental Congress also established the Secret Committee. This clandestine committee arranged for American privateers to purchase and smuggle arms to the United States. The committee used large sums of money to pay for weapons, and additionally solicited aid from Britain's numerous European rivals. The world of the Secret Committee began in 1775, amassing weapons while still under British rule. After the Declaration of Independence was signed, the committee burned its papers

and transaction ledgers to protect their contacts in case the colonies lost their bid for sovereignty.

The smuggling of weapons proved a successful venture. The United States armed its troops within months, although supplies remained limited throughout the course of the war. Many American leaders, including Thomas Jefferson, ran successful privateering ventures, using their wealth and diplomatic contacts abroad to smuggle arms for the war effort. American privateers ran their illegal cargo through the British blockade under the guise of foreign named vessels and foreign flags. Patriot spies also learned the new British semaphore code, enabling blockade runners to falsely identify themselves as British ships.

The first United States counterintelligence operations were directed by the Commission for Detecting and Defeating Conspiracies. The commission endowed several groups, mostly in New York and Philadelphia, with the task of apprehending British spies. The organization was the nation's first secret service, employing local militia under its command to help ferret out suspected traitors and enemy spies. The group used the criteria defined by the Committee on Spies when identifying, trying, and sentencing suspects. The rules of the committee, incorporated into the Articles of War in 1776, defined the crimes of treason and espionage during the course of war, and shaped the American intelligence community with its strict definitions of intelligence information, espionage acts, conspiracy, and aiding the enemy.

Espionage

Although the secret committees of the Second Continental Congress were the first national organizations to address intelligence issues, individuals and civilian spy networks carried out the most vital American intelligence operations of the Revolutionary War.

Robert Townsend used his position as a prominent merchant in British-occupied New York to gather intelligence information on behalf of the American government. Townsend operated a significant spy ring, known as the Culper Ring. The ring employed both men and women, and based its operations in New York and Long Island. Most members of the espionage group used their professions as cover, relying on customers and patrons from the British military to divulge information about British military operations voluntarily. Several member of the Culper Ring were caught by British occupation authorities, but the ring never stopped feeding information to American authorities during the war.

Major John Clark established and administered a similar espionage group in Philadelphia. Clark and his group fed General George Washington critical information and supplies while his troops wintered at Valley Forge. The Clark Ring obtained detailed information about British defenses , supply lines, and battle plans, allowing the American Patriot forces to plan a series of successful surprise attacks, breaking the British stronghold in the region and paving the way to seize control of Philadelphia.

Several other Patriot civilian espionage rings operated across the country and in Britain. Individual civilians most often contributed to counterintelligence measures by posing as Loyalists and infiltrating British-sympathizing groups. Enoch Crosby and John Honeyman both infiltrated several pro-British organizations and delivered valuable intelligence information about the planned use of Hessian mercenaries in British military operations.

Within the military, espionage operations were often tailored to fit the strategic needs of the battlefield. Scouts, many of whom were American Indians, reported on the location and strength of British military instillations and encampments. The first recorded American military agent of espionage was Nathan Hale. After a crushing defeat at the Battle of Long Island, Washington called for a volunteer to spy on the British and report to the American command with details of future battle plans. Hale volunteered, but was later captured behind enemy lines and hanged.

Covert actions and special operations. Most American, government-backed espionage actions against the British were covert, strategic operations of deception or sabotage. Blockade running was of critical importance to the American war effort. Though British ships clogged United States harbors, American privateers successfully ran British blockades to provide troops with supplies, ammunition, and even supporting troops from France.

The American government, usually through diplomats abroad, employed a number of agents to sabotage wartime industries in Britain. Munitions factories, shipyards, and weapons storage facilities were the main targets of Patriot sabotage. Twelve separate targets were attacked in London and Portsmouth in a three-year period by one American saboteur before the agent fell into British custody and was executed.

Some operations of deception were more insidious. British troops, wanting to keep some local Indian populations from joining the American cause, bribed village leaders with gifts of blankets and jewelry. Earlier, they gave the Indians blankets from their military sick wards, often infected with smallpox. The disease continued to devastate the American Indian population during the course of the war. Both British and American military personnel traded contaminated goods through Indian trade networks, hoping the goods would fall into enemy hands.

Codes, cryptology, and secret writing. American and British forces employed codes and ciphers to disguise their communications, and took precautionary measures to ensure that crucial messages were not intercepted by the enemy.

Both armies employed replacement codes, where pre-set letters or words replaced other letters or words in communications. This required intense memorization of static codes, or the use of codebooks, which had a high risk of being stolen by rival spies. The codes used in the American Revolution were simple and easy to decipher, permitting both armies to read intercepts with relative ease. In 1777, the Americans unveiled a new mathematical code that remained unbroken throughout the war, but the complexity of the code precluded its daily use and limited its effectiveness to overseas diplomatic dispatches that did not have to be deciphered in a timely manner.

In lieu of complex codes, American cryptologists developed and used secret writing techniques. Disappearing inks are an ancient espionage trick, but during the Revolution, American scientists developed several inks that needed a series of reagents to reveal the hidden message. Some of these inks were waterproof and held up for months in difficult conditions, a necessity for warfare across wild and vast terrain. To further disguise messages, agents were instructed to write their communications between the lines of common publications, such as pamphlets and almanacs.

Intelligence operations abroad and at sea required further technological advances in espionage tradecraft. With the British blockade, American agents had to be ready to conceal or destroy intelligence information that they carried. To preserve and conceal information, agents developed small, silver containers in which information could be hidden. The container could then be thrown into the fire and melted or be swallowed by the agent, permitting to information to possibly remain intact and undetected.

After the end of the Revolution, and the establishment of an independent United States government, most military and espionage institutions were dissolved. Until the outbreak of World War I in 1914, American intelligence agencies and services were exclusively wartime organizations, rapidly assembled in times of conflict, and dissolved in times of peace. Though intelligence operations certainly aided the victory of American forces over the larger and better-armed British military, peacetime intelligence remained scattered, and largely focused on political and diplomatic espionage operations.

■ FURTHER READING:

BOOKS:

Finn, Elizabeth. *Pox Americana.* New Haven, CT: Yale University Press, 2000.

Mahoney, Harry Thayer, and Marjorie Locke. *Gallantry in Action: A Biographic Dictionary of Espionage in the American Revolutionary War.* Lanham, MD: University Press of America, 1999.

ELECTRONIC:

Central Intelligence Agency. "Intelligence in the War of Independence."<http://www.odci.gov/cia/publications/warindep/frames.html> (May 19, 2003).

SEE ALSO

War of 1812

RF Detection

Among the most potentially damaging weapons of electromagnetic warfare are RF, or radio frequency systems. Also known as directed-energy weapons, these use electromagnetic energy on specific frequencies to disable electronic systems. There exist means to protect against directed-energy weapons; aside from "hardening" computer systems, protection is possible through the employment of electronic RF detection equipment, which operates on a principle similar to that of radar.

In the modern world of sophisticated, computerized fighter jets, the missile systems of one fighter aircraft can only "lock on" and fire on an enemy craft if the enemy has his radar systems activated. The same electronic radio-frequency system that allows a plane to navigate also makes it capable of being tracked electronically across the sky. Similarly, that which makes RF weaponry so potentially threatening—the fact that they can disable flight systems by interfering with vital frequencies on the electromagnetic spectrum—also makes them detectable.

Given the fact that Soviet and Russian technicians have reportedly developed RF weaponry, it is assumed that technicians working for the United States Department of Defense have created RF detection equipment at least as sophisticated. At a much lower end are civilian and consumer versions of computerized RF detection equipment, retailing for a few hundred or thousand dollars. A January 2003 article in the *Wall Street Journal* described a pocket wireless system called Spotme that could read electronic badges on guests at a party and provide the user with other guest's names, photographs, and contact information. For security purposes, there are RF detection consoles that operate across a wide frequency spectrum to search out and identify potentially harmful RF sources.

■ FURTHER READING:

PERIODICALS:

Fund, John. "In the Fray: People Spotters—European Gizmo Tells Who's Who." *Wall Street Journal.* (January 23, 2003): D8.

Torregrosa-Penalva, German, et al. "Microwave Temperature Compensated Detector Design for Wide Dynamic Range Applications." *Microwave Journal* 44, no. 5 (May 2001): 336–346.

SEE ALSO

Electronic Warfare

RADAR
Radio Frequency (RF) Weapons

Ricin

JULI BERWALD

Ricin is a highly toxic protein that is derived from the bean of the castor plant (*Ricinus communis*). The toxin causes cell death by inactivating ribosomes, which are responsible for protein synthesis. Ricin can be produced in liquid, crystal or powdered forms, and it can be inhaled, ingested, or injected. It causes fever, cough, weakness, abdominal pain, vomiting, diarrhea, dehydration, and death. There is no cure for Ricin poisoning, and medical treatment is simply supportive.

Chemical structure and pathological pathway. Ricin is a protein composed of two hemagglutinins and two toxins (RCL III and RCL IV). The toxins are made up of an A polypeptide chain and a B polypeptide chain, which are joined by a disulfide bond. The general molecular structure of Ricin is similar to other biologically produced toxins, such as botulinum, cholera, diptheria, and tetanus.

The B portion of Ricin binds to glycoproteins and glycolipids that terminate with galactose on the exterior of cell membranes. Ricin is then transported inside the cell by endocytosis. Once inside the cytosol of the cell, the A portion of the molecule binds to the 60S ribosome, stopping protein synthesis. A single molecule of Ricin can kill a cell.

Ricin poisoning. Ricin poisoning can occur by dermal (skin) exposure, aerosol inhalation, ingestion, or injections, and the symptoms vary depending on the route of exposure. If Ricin comes in contact with the skin, it is unlikely to be fatal, unless combined with a solvent such as DMSO. Aerosol inhalation of Ricin can cause symptoms within four to eight hours. Fever, chest tightness, cough, nausea, and joint pain may occur. Ricin can cause cell death in the respiratory system and eventual respiratory failure. If Ricin is ingested, it can cause severe lesions in the digestive system within two hours of exposure. It may cause abdominal pain, nausea, vomiting, and bloody diarrhea. Eventual complications include cell death in the liver, kidney, adrenal glands, and central nervous system. Injection of Ricin causes local cell death in muscles, tissue, and lymph nodes. Ricin poisoning causes death generally within three to five days. If Ricin exposure does not cause death within five days, the victim will probably survive.

There is no cure for Ricin poisoning, although a vaccine is currently under development. Treatment for dermal exposure includes decontamination using soap and water or a hypochlorite (bleach) solution, which deactivates Ricin. In case of aerosol inhalation, treatment is the administration of oxygen, intubation, and ventilation. Ingestion of Ricin is treated with activated charcoal.

Ricin production and use as a biological weapon. Ricin comes from castor beans, which produce castor oil, a component of brake fluid and hydraulic fluid. One million tons of castor beans are processed each year and the resulting waste mash contains 5–10% Ricin. The 66,000 Dalton protein can be purified from the mash using chromatography. Once purified, Ricin is a very stable molecule that is able to withstand changes in environmental conditions.

Ricin is considered moderately threatening as a biological warfare agent. Although it is environmentally stable, relatively easy to obtain, highly toxic, and has no vaccine, it is not communicable like other biological agents such as anthrax and smallpox. Ricin is most often considered a threat as a food or water contaminant. A large amount would be required to cover a significant area.

The most famous case involving Ricin is the assassination of the Bulgarian dissident Georgi Markov. In 1978, Markov was working in London as a British Broadcasting Company (BBC) correspondent. As he was walking across Waterloo Bridge, a man jabbed the tip of an umbrella into Markov's right thigh, murmured an apology, and slipped away into the crowd. Markov died four days later. After the collapse of the Soviet Union, the new Bulgarian government admitted that their Secret Service had been responsible for the murder. The KGB produced the murder weapon: an umbrella modified to inject a 1.7 mm platinum pellet filled with Ricin into Markov's leg.

Incidents involving Ricin have occurred in the United States. Four men were convicted of plotting to kill a United States marshal with Ricin in Minnesota in 1991. They were all members of an extremist antigovernment group called the Patriots Council. In 1995, Canadian officials stopped Thomas Lavey at the border with Alaska with a bag of Ricin. He was also in possession of guns, ammunition, manuals for making biological and chemical weapons, and neo-Nazi literature.

Ricin has been loosely linked to the al-Qaeda terrorism network. In January 2002, police in London were advised that of a group of men were manufacturing Ricin in their apartment. Although only a small amount of Ricin was found, castor beans as well as equipment for crushing and extracting Ricin from the beans were discovered. Seven men of North African background were arrested in the incident, and security experts speculate that they had links to al-Qaeda. There also are reports that Ricin was found in caves abandoned by the Taliban in Afghanistan.

■ FURTHER READING:

BOOKS:

Haugen, David M., ed. *Biological and Chemical Weapons.* San Diego: Greenhaven Press, Inc., 2001.

Sifton, David W., ed. *PDR Guide to Biological and Chemical Warfare Response.* Montvale, NJ: Thompson/Physician's Desk Reference, 2002.

Wise, David. *Cassidy's Run: The Secret Spy War over Nerve Gas.* New York: Random House, Inc., 2000.

ELECTRONIC:

Animal Science at Cornell University. "Ricin Toxin From Castor Bean Plant." <http://www.ansi.cornell.edu/plants/toxicagents/Ricin/Ricin.htm> (February 5, 2003).

BBC News UK "Seventh Arrest in Ricin Case." <http://news.bbc.co.uk/1/hi/uk/2637515.stm> (February 5, 2003).

Medical NBC Online. "Ricin." <http://www.nbc-med.org/SiteContent/RedRef/OnlineRef/FieldManuals/medman/Ricin.htm> (February 5, 2003).

Mirarchi, Ferdinando L., eMedicine. "Ricin." <http://www.emedicine.com/emerg/topic889.htm> (February 5, 2003).

SEE ALSO

Biological Warfare
Bioterrorism
Toxins

Robotic Vehicles

■ JUDSON KNIGHT

From the late 1980s onward, robotic vehicles have become an increasingly important component of security operations and related activities. They can be used to gather information in areas where a human could not safely go and undertake tasks a human could not safely perform. Robotic vehicles can be used, for instance, in underwater minesweeping, and in sites contaminated by nuclear, biological, or chemical materials. The use of robotic vehicles on scientific expeditions to such inhospitable locales as the polar ice cap and the surface of Mars portends a variety of applications for intelligence gathering. Robotic technology also has uses in energy harvesting, or the gathering of energy from ambient sources such as sunlight, wind, or barometric fluctuations.

Robotic Operation

A 1994 article in *The Industrial Robot* identified five parameters or "subtasks" of robotic operation: localization, motion control, mapping, path planning, and communication with the operating station. The subtask of localization is a matter highly analogous to human movement. If a person does not know his or her location, that person cannot know where he or she is going; in order to stay on the right path, it is necessary to receive continual data regarding the environment. For the human mind, these skills are largely automatic—one does not have to think about walking around an obstacle, for instance—but for the robot, course correction must be built into the overall operating system.

Closely related to the problem of localization is that of motion control. Some robots operate on set paths analogous to a railroad track, but as technology has progressed, scientists have developed means that will allow robotic vehicles to operate in a less modified environment, using navigational markers. These markers are reflective targets that serve as beacons, allowing the robotic vehicle to correct its course when it strays from a desired path. Efforts to make these vehicles capable of operating in a completely unrestricted environment are ongoing.

Also closely related to localization is the issue of mapping the environment—a function that, once again, is automatic for humans. Robots use visual, ultrasonic, and touch sensors. More sophisticated machines made for operating in an outdoor locale have means of navigating by visual methods using focus-enhancing technology.

Robotic scientists are using ever more sophisticated means of navigation. Among these is the use of a camera to provide data allowing the home station to implement course correction measures. The Global Positioning System, or GPS, also offers a method of aiding navigation in large, open environments. Still more complex are various techniques applying teleoperation through virtual-reality systems.

Path planning and communication. Path planning involves addressing the problem of minimizing the output of time or energy required to reach a certain goal. In spatial terms, path planning involves helping the robot to find the shortest possible distance between two points. Temporal or time-based path planning may be more challenging in view of unpredictable inputs from the environment.

Finally, there is the matter of communication with the home station, a problem encountered by humans in tasks ranging from intelligence gathering to space travel. In addition to receiving information on changing courses or tasks, robots undertaking sophisticated activities may need to send back video data or other forms of intelligence.

Uses for Robotic Vehicles

The applications, and potential applications, of robotic vehicles are myriad. Within the realm of industry, they can be used for everything from moving containers in ports (an application demonstrated in 1994) to clearing snow off of airport runways. On a consumer level, robotic technology can be employed in wheelchairs and in cleaning homes or offices.

In the realm of scientific study, robotic vehicles provide a means of conducting research in environments that

A British Army robot inspects a suspect vehicle for explosives outside the Europa Hotel in Belfast, Northern Ireland. AP/WIDE WORLD PHOTOS.

are either presently or forever inaccessible to humans. The use of a robotic vehicle to collect data during the 1997 National Aeronautics and Space Administration (NASA) Mars Pathfinder Expedition gained widespread attention, but scientists also use robots much closer to home. Small, submarine-like robots known as autonomous underwater vehicles (AUVs) have in some cases taken the place of acoustic remote-sensing technology to map seabed topography. They also offer promise in areas impenetrable to more traditional methods—for instance, for mapping hydrothermal vents beneath the Arctic Ocean.

Security and related activities. Applications for robotic technology in security and related functions are fast emerging. At the simplest level, a robotic vehicle "walking a beat" could be used to patrol a parking garage by providing real-time video data to a facility security station. The U.S. Navy in the 1980s began using AUVs to conduct minesweeping operations in the Persian Gulf. In 1996, scientists at Lawrence Livermore National Laboratory created a prototype for a robotic vehicle that could be outfitted for a variety of tasks, including not only mine detection and clearance, but also intelligence-gathering.

In 2000, *Design News* reported that technicians at Sandia National Laboratory were in the process of developing a highly sophisticated machine called a MARV, or miniature autonomous robotic vehicle. Very small—a cubic inch (16.4 cc) in size—the MARV is designed to "rove in packs" for purposes such as surveying a contaminated area, sweeping for and disabling mines, or locating biological weapons. Engineers at Sandia have addressed the problem of course correction through genetic algorithm-based software, a fascinating innovation intended to mimic the functions of a human brain.

Energy harvesting. An area of research in which robotic technology plays a dual role, both as a tool and as a potential beneficiary, is energy harvesting. The latter is the gathering of energy from ambient sources, including sunlight, wind, wave action, water currents, geothermal components such as volcanoes, chemical and thermal gradients, barometric fluctuations, electromagnetic radiation, and human and other biological systems. The aim of energy-harvesting efforts using robotic technology and other means is to increase the efficiency of power delivery by a factor of 10 with respect to conventional systems.

The U.S. Defense Advanced Research Projects Agency (DARPA) has expressed an interest in developing robotic technology for the purposes of energy harvesting, as well using energy-harvesting methods to supply power to robotic vehicles. In 1997, DARPA allocated $25 million toward energy-harvesting projects, among which was a

robotic "boot" (functional by 2001) that harvests energy from walking.

In 2002, engineers at Pennsylvania State University introduced an optimized energy-harvesting circuit capable of improving retrieval systems from vibration—including that of machine operation and human motion—by a factor of four. Among the applications for this energy-harvesting technology, researchers noted, were robotic control and guidance systems to be used in manufacturing and other activities.

FURTHER READING:

PERIODICALS:

"Circuit Transfers Four Times More Power out of Vibration." *Resource* 9, no. 11 (November 2002): 6.

"Designed for Danger." *Design News* 55, no. 2 (January 17, 2000): 28.

"EDM on Mission to Mars." *Manufacturing Engineering* 119, no. 4 (October 1997): 116.

Evers, Stacey. "DARPA to Reap Benefits of 'Energy Harvesting'." *Jane's Defence Weekly.* (November 26, 1997): 8.

Jarvis, Ray. "Robot Navigation." *The Industrial Robot* 21, no. 2 (1994): 3.

"Novel Design of Countermine Robot." *Jane's International Defense Review* (February 1, 1996): 20.

"Robo P.I." *American Scientist* 90, no. 1 (January/February 2002): 28–29.

Treherne, Jan. "Robotic Roads—Pathways to the Future." *The Industrial Robot* 21, no. 5 (1994): 3.

ELECTRONIC:

Energy Harvesting. Defense Advanced Research Projects Agency. <http://www.darpa.mil/dso/trans/energy/> (April 15, 2003).

SEE ALSO

DARPA (Defense Advanced Research Projects Agency)
GPS
NASA (National Air and Space Administration)
Unmanned Aerial Vehicles (UAVs)

Romania, Intelligence and Security

A former Soviet bloc country, Romania is struggling to rebuild its national government and economy following the collapse of Soviet communism. Romania further struggled to free its government of authoritarian influences. In 1989, nationalist forces arrested, tried, and executed dictator Nicolae Ceausescu, beginning the arduous process of democratizing the Romanian government. During Ceausescu's rule, Romanian intelligence and security forces conducted a brutal campaign to crush political dissent. The government now endeavors to distance Romania's new intelligence and security community with the legacy of its predecessors. However, lingering public suspicion of government agencies and police forces has proved difficult to overcome.

The Office of the President oversees Romania's primary domestic intelligence and security services. The Romanian Intelligence Service (SRI) is the nation's main internal intelligence agency. The agency is responsible for assessing threats to national security, conducting surveillance on behalf of the military and government, and protecting national economic interests. Though the agency has been reformed several times since 1990, public suspicion about the secretive nature of domestic intelligence policy persists. Parliamentary restrictions place on the SRI include the necessity to obtain warrants for most surveillance operations, and a permanent ban on using intelligence service equipment and personnel for political reasons. To help assuage public concerns, the SRI is one of two Romanian intelligence agencies whose organization and operation is subject to parliamentary review.

The SRI works closely with the Guard and Protection Service (SSP), a national law enforcement agency. The SSP is charged with the protection of government officials and foreign diplomats. In cooperation with the Romanian Intelligence Service, the SSP functions as a special action unit for anti-terrorism operations.

The Ministry of the Interior controls Romania's civilian intelligence community. Known as the Securitate, the Department of State Security was the communist-era intelligence agency that worked with the secret police forces to conduct domestic espionage. Post-Cold War democratic reforms dissolved the Securitate and created new agencies, none of which are authorized to conduct espionage activities on Romanian citizens. The Interior Ministry Intelligence Directorate (UM 0251) now directs civilian intelligence and security service operations. The agency is charged with protecting national security. The Gendarmerie, the national police force, aids Romanian intelligence services to insure public safety.

Foreign intelligence is coordinated through the Ministry of Foreign Affairs (MAE). The Ministry employs its own intelligence force, the Foreign Intelligence Service (SIE). The SIE analyzes external threats to Romanian interests.

The Romanian military operates its own intelligence forces in specially trained units. The Ministry of National Defense coordinates some military intelligence operations through various operational branches. The Special Telecommunications Services specializes in communications security. The Counter-Intelligence Directorate oversees military, and sometimes civilian, counterintelligence operations. The Intelligence Directorate of the Army also operates within the Ministry of National Defense,

coordinating operations to assess and preserve national security using military intelligence resources.

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union
European Union

Room 40

ADRIENNE WILMOTH LERNER

Advances in communications technology such as the telephone and trans-Atlantic telegraph prompted the development of increasingly sophisticated cipher systems and codes. The telegraph facilitated communication between command and remote forces, but the lines were vulnerable to tapping, the interception of message traffic, on the wires. As codes became more mathematical and complicated, intelligence services enlisted professional cryptologists, or code breakers, and language translators.

At the outbreak of World War I in 1914, British intelligence began intercepting wire transmissions sent by the German military and government. The German cipher was unknown, so British intelligence quickly established a cryptography department to begin the task of breaking enemy code. The department, under the direction of intelligence officer Reginald "Blinker" Hall and code expert Alfred Ewing, was located in Room 40 of the Admiralty Building. The cryptology department housed in Room 40 was only a small branch of Britain's large intelligence system. However, after remarkable successes achieved by the team, Room 40 became a catch-all nickname for British military intelligence during the war.

While the cipher systems themselves were becoming more complex in the early twentieth century, the technology to decode them had not advanced at the same pace. Codes were still worked out by hand in long sequences to look for mathematical permutations and deviations from known ciphers that formed essential code patterns. The best means of breaking code was to capture an enemy codebook. Beginning in 1914, an extraordinary string of events led to the capture of not one, but three different German code books, allowing Room 40 to intercept, decode, and translate most German military and diplomatic transmissions.

Early in the war, a box recovered from a sunken German submarine yielded a copy of the German Foreign Office codebook. British intelligence was thus able to monitor diplomatic correspondence between the German government and its territories and embassies. Similarly fortuitous for Room 40, later that year a German cruiser was sunk by the Russian Navy. When the Russian fleet rescued surviving German sailors from the downed ship, one officer was found to have a copy of the German Naval codebook. The codebook was sent to British intelligence, and Room 40 was able to decipher wire traffic from German fleet commanders and ships. As most ships in the German fleet reported their positions daily, British intelligence learned individual ship identification codes and tracked the position of most German warships and submarines by the end of 1915.

While the two recovered codebooks let British military intelligence decipher nearly a quarter of German military transmissions, the capture of a third codebook in 1915 gave Room 40 the mathematical key to German cipher system. Wilhelm Wassmuss, the German consul in Persia, hastily fled his office to escape encroaching British forces, leaving behind his copy of the German diplomatic codebook. Room 40 cryptographers discovered that the first two codebooks recovered were standard permutations of the third code. Thus, several German codes were based on a single cipher system and, by applying systematic variations, British cryptographers were able to break the remaining codes.

In 1917, Room 40 had its greatest success. The United States, while holding Allied sympathies and aiding the transportation of ammunition across the Atlantic Ocean, held fast to a policy of non-intervention in the war. Increased German submarine warfare, the sinking of U.S. and Allied merchant and passenger ships, and the work of German saboteurs in the Black Tom explosion fostered a shift in American attitudes toward entering the war. On the morning of January 17, 1917, British military intelligence intercepted secret communication from German Foreign Minister Arthur Zimmerman to the German ambassador in Washington, D.C. The message took cryptographers nearly a month to decode in whole, but the importance of the telegram was realized almost immediately. The Zimmerman Telegram, as it became known, revealed German plans to begin unrestricted submarine warfare in the Atlantic. Knowing that this could bring America into the war, Germany planned to make alliances with Mexico and Japan to keep the U.S. occupied on its own ground instead of in Europe. The telegram not only spoke of driving England to surrender, but also promised Mexico the return of its former territories in Texas, New Mexico, and Arizona. British intelligence shared the contents of the memo with the American government, thwarting the German plan. Declaring war on Germany shortly after, America entered the war in Europe.

In 1918, Room 40 intercepted transmissions that revealed that a sizable group of German sailors had mutinied. News of a German surrender soon followed. The triumphs of Room 40 during the course of World War I convinced the British Admiralty that cryptography was a necessary tool of modern warfare. By the advent of World War II, however, the field of cryptography significantly changed with the introduction of cipher machines, teleprinters, and radio.

SEE ALSO

Black Tom Explosion

World War I
World War I: Loss of the German Codebook

Rosenberg (Ethel and Julius) Espionage Case

ADRIENNE WILMOTH LERNER

Julius and Ethel Rosenberg were a couple accused in 1950 by the United States government of operating a Soviet spy network and giving the Soviet Union plans for the atomic bomb. During a time of tense scrutiny over alleged communist infiltration of the American government, the trial of the Rosenbergs became the center of a political storm over communist influence in America. Their trial was one of the most controversial of the twentieth century, ending with their execution.

Julius Rosenberg was a committed communist who had graduated from the City College of New York in 1939 with a degree in electrical engineering. He married Ethel Greenglass in the summer of that year. She was a headstrong woman, active in organizing labor groups. Julius had opened a mechanic shop with his brother-in-law, but the business soon began to fail, largely due to lack of attention by Julius, who invested his time spying for the Soviets. He began by stealing manuals for radar tubes and proximity fuses, and by the late 1940s, had two apartments set up as microfilm laboratories.

The arrest of the Rosenbergs was set in motion when the FBI arrested Klaus Fuchs, a British scientist who gave atomic secrets to the Soviets while working on the Manhattan Project. Fuchs's arrest and confession led to the arrest of Harry Gold, a courier for Soviet spies. Gold in turn led investigators to David Greenglass, a minor spy who confessed quickly. Greenglass then accused his sister Ethel and brother-in-law Julius of controlling his activities.

Julius immediately realized the implications of Harry Gold's arrest and began to make arrangements to get out of the country, but the FBI moved swiftly. Julius Rosenberg was arrested in July 1950.

Ethel Rosenberg was later arrested in August. Although Federal investigators had little evidence against her, they hoped to use the threat of prosecuting her as a lever to persuade Julius to confess. The plan failed, and the couple was charged with conspiracy to commit espionage. Their trial began on March 6, 1951.

From the beginning, the trial attracted national attention. The prosecution decided to keep the scope of the trial as narrow as possible, with establishing the Rosenbergs' guilt the main target, and exposing their spy ring a lesser concern. Nonetheless, the trial was punctuated by numerous arrests of spies associated with the Rosenbergs, some appearing in court to testify against them.

Ethel Rosenberg and her husband Julius are separated by a wire screen as they ride to separate jails in New York City in 1951 after their conviction for delivering secrets, including vital atomic bomb data, to the Soviet Union. AP/WIDE WORLD PHOTOS.

The defense tried to downplay the importance of the information the prosecution claimed the Rosenbergs had stolen, but then turned around and requested that all spectators and reporters be barred from the courtroom when the information was discussed.

The Rosenbergs accused David Greenglass of turning on them because of their failed business, but these efforts only elicited sympathy for a man who had been forced to turn in a family member. Greenglass damaged the Rosenbergs by testifying that Julius had arranged for him to give Harry Gold the design of the atomic bomb used on Nagasaki (which differed considerably from the Hiroshima bomb). When Gold himself testified, he named Anatoli Yakovlev as his contact. This directly tied the Rosenbergs to a known Soviet agent. Julius and Ethel Rosenberg were found guilty on several accounts of espionage and conspiracy. They were sentenced to execution, a sentence usually reserved for cases of treason.

After months in prison, the Rosenbergs still maintained their innocence and began to write poignant letters, which were widely published, protesting their treatment. The case was followed closely in Europe, where many felt the Rosenbergs were being persecuted because they were Jewish (though Judge Kaufman was also Jewish). A movement began to protest the "injustice" of the Rosenberg

trial. Passions both for and against the Rosenbergs grew so great that they even threatened Franco-American relations, as the French were particularly harsh in their condemnation of the trial as a sham.

In the months between the sentencing and execution, criticism of the trial grew more strident, and major demonstrations were held. Nobel-prize winner Jean-Paul Sartre called the case "a legal lynching which smears with blood a whole nation." In spite of attempts at appeal and a temporary stay issued by Supreme Court Justice William O. Douglas, Julius and Ethel Rosenberg were executed on June 19, 1953, both refusing to confess.

Years after the event, the case continues to stir debate. Although the Rosenbergs were communists and engaged in espionage, they did not spy for an enemy of the United States, as the sentence might indicate, but rather for its wartime ally. Recent studies of the couple's activities show that the evidence against them was overwhelming. The declassification and release of Venona transcripts (a secret, decades-long, general surveillance operation) further implicated the Rosenbergs. Regardless of the evidence, the political and social upheaval surrounding the trial, and its ultimate outcome, can only be understood through the lens of heightened Cold War tensions and anti-Communist hysteria.

■ FURTHER READING:

BOOKS:

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today.* M.Evans, 1997.

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
McCarthyism

Russia, Intelligence and Security

The Russian Empire dominated Eastern Europe and Western Asia from the Middle Ages through the nineteenth century. However, the devastation caused by World War I plunged the nation into revolution in 1917, leading to an overthrow of the Czarist regime and the birth of communism. The communist government created a large intelligence community, with secret police forces, to conduct political espionage on ordinary citizens. The era was marred by political show trials and the harsh imprisonment of political dissidents. Before the outbreak of World War II, the oppressive regime of Joseph Stalin centralized the nation's agricultural and industrial systems. Despite the rapid industrialization and growth of the national military infrastructure, the ensuing economic turmoil, brutal political oppression, and famine cost millions of lives.

Russia entered World War II as a member of the Allied forces. Their participation in the war effort was key to the Allied defeat of Germany in 1945. Although Russia was a strategic wartime ally, relations between Russia and the West, particularly the United States, quickly soured in the first post-war months. The diplomatic, economic, and military standoff between the United States and Russia intensified into the decades-long Cold War. The nations engaged in an intelligence war in lieu of military conflict, and the antagonism between the two states redefined their national intelligence services and modern espionage tradecraft.

Hard-line communism fell out of favor in Russia as the national economy plummeted in the 1980s. A period of détente between Russia and the West allowed General Secretary Mikhail Gorbachev to implement a series of political and economic reforms, known as Glasnost and Perestroika. Reforms were also made to the national intelligence super-agency, the KGB. Though the leader sought to modernize the face of communism, the reform programs sped the regime's eventual downfall. The Soviet Union splintered in 1991. The largest former province, and the heart of the old Russian Empire, became the Russian Federation. Since the creation of the democratic republic, the nation has struggled to reform its national political system and it intelligence community.

Since the breakup of the Soviet Union, Russia's intelligence and security agencies have been administered, and influenced, by the Office of the President of the Russian Federation. The executive branch governs the intelligence community via the Russian National Security Council, and the Defense council. The two boards act as a liaison between the government and the intelligence services, briefing the executive and legislature when national security threats arise. Since the Russian intelligence community is now more departmentalized than it was under Soviet control, the two councils help to centralize the dissemination of intelligence information and the formation of intelligence policy.

The *Federal'naya Sluzhba Bezopasnosti*, Federal Security Service (FSB), a successor agency of the Soviet KGB and Russian Federal Counterintelligence Service (FSK), is Russia's counterintelligence agency. FSB operations focus on domestic counterespionage and internal security. Headquartered in Lubyanka, the agency employs over 75,000 people. Since the creation of the agency, the Russian government has placed increasing limitation on FSB operations to guard against abuse of intelligence community resources. Russian law now severely restricts FSB surveillance operations conducted against ordinary citizens, and new constitutional reforms seek to prohibit the use of FSB forces for political espionage.

In response to the growth of organized crime after the dissolution of the Soviet Union, the Russian intelligence community established the Main Administration for Organized Crime (RUOP). The agency uses human and remote intelligence to infiltrate and investigate crime syndicates operating within Russia's borders. Despite ongoing efforts of the agency, organized crime has increased in Russia.

Russian intelligence operates special assignment bureaus in Kaliningrad and Chechnya. The Russian military's involvement in the region, and endemic conflict between nationalist and Russian factions, prompted the intelligence community to form task forces devoted to counterterrorism and counterintelligence. These operational units are usually a mix of civilian and military intelligence personnel and report to a variety of agencies, including the FSB and the Russian Security Council.

Though Russia has attempted to distance its new intelligence community from the legacy of the Soviet KGB and internal secret police forces, many of its new national intelligence agencies are indeed successor organizations of specialized departments within the former KGB. The Foreign Intelligence Service (SVR) was one of the first operational departments of the KGB to emerge as its own intelligence entity. The SVR now oversees most of Russia's foreign intelligence operations, including collection and analysis of data. The main intelligence objectives of the SVR are to collect information on rival military and economic powers. In 1995, the head of the SVR claimed that expansion of the North Atlantic Treaty Organization (NATO) was the largest threat to Russian sovereignty and regional influence. In response to the perceived threat, the SVR conducts routine foreign intelligence surveillance of the former Soviet republics.

In the late 1990s, the focus of SVR operations shifted from military-related foreign intelligence to industrial, scientific, and technological espionage. Several divisions within the SVR use extensive human and remote intelligence networks to collect information on rival economies. Russian intelligence operated its own intelligence gathering missions in Asia and the West, but also devoted considerable resources to counterintelligence in a bid to protect Russian industry. The rise of the European Union (EU) prompted Russia to take a more strident political stance on international trade laws. However, in 2000, the nation refused to join a UN Security Council-led effort to limit economic espionage and prosecute industrial spies.

Russia's misleadingly named Main intelligence Agency (GRU) is the nation's primary intelligence information clearinghouse and analysis bureau. Though the agency does conduct intelligence gathering missions, its primary duty is to coordinate inter-agency information operations and process intelligence materials.

Russia garnered international criticism for its lack of security and protective intelligence measures against the proliferation of weapons from the former Soviet Union. Russia now devotes considerable intelligence resources to international non-proliferation efforts. However, national intelligence and security services have had little efficacy against criminal organizations and individuals selling arms and weaponry to terrorist groups and rogue states.

Russian foreign policy continues to evolve. Despite hostilities toward EU and NATO expansion, the Russian government has cooperated with European and United Nations anti-terrorism efforts. In 2003, Russia, with the diplomatic cooperation of France and Germany, moved to block UN-sanctioned military action against Iraq.

FURTHER READING:

ELECTRONIC:

CIA World Factbook. "Russia" <http://www.cia.gov/cia/publications/factbook/geos/rs.html>(May 5, 2003).

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*

Russian Nuclear Materials, Security Issues

MICHAEL J. O'NEAL

The breakup of the former Soviet Union in 1991 raised fears about the disposition and security of that nation's nuclear materials, including its strategic and tactical nuclear weapons. Of more immediate concern is the security of Soviet stores of plutonium and enriched uranium, which could be used to make either nuclear weapons or "radiological dispersal devices" (RDDs), or "dirty bombs"—conventional explosives that would spew radioactive debris packed around them over a wide area. Since 1991, the United States has provided financial and technical assistance to help Russia and other former Soviet states secure these materials.

Background. During the cold war, the Soviet Union, like the United States, amassed an imposing stockpile of nuclear weapons. Western estimates were that by 1991 the Soviets had in excess of 27,000 nuclear weapons—at least 11,000 strategic weapons on land-based intercontinental ballistic missiles (ICBMs) and at least 15,000 warheads for tactical weapons such as artillery shells and cruise missiles. Later information suggested that the total might

have been as high as 45,000 warheads. Additionally, the Soviets had as much as 1,200 metric tons of weapons-grade uranium and 160 metric tons of plutonium, enough to triple their stockpile of nuclear weapons. Eighty percent of the strategic weapons were deployed at bases in Russia, but the remainder were deployed in the Soviet republics of Ukraine, Belarus, and Kazakhstan. Tactical nuclear weapons were deployed closer to potential theaters of operation, including Eastern Europe and the former Baltic republics. Still others were deployed in Armenia, Azerbaijan, Belarus, Ukraine, Kazakhstan, Georgia, and the Central Asian states (Kirghizia, Tajikistan, Turkmenistan, Uzbekistan).

While these nuclear materials were under the command and control of Soviet authorities in Moscow, the chief threat they posed to the West was strategic: They could be used against the West in a nuclear exchange. Regardless, in contrast to the modern situation, Soviet authorities maintained account of these materials and security around nuclear facilities was tight. Weapons could be fired only through a central command authority. Although an enemy to the West, the Soviet regime was at least a politically stable state that could be anticipated act rationally in its own self-interest, and which was unlikely to allow the use of nuclear materials for terrorist purposes. Essentially, the threat that nuclear materials posed to the West was predictable, manageable, and able to be reduced through negotiation and arms-control treaties.

The status quo began to change in the 1980s. The Soviets were finding it increasingly difficult to maintain control over an enormous empire that stretched from the German border to Asia. They also faced increasingly restive ethnic and national populations demanding self-determination. Under these pressures, the Soviet Union began to disintegrate and finally collapsed in late 1991. By then, the Soviets had retrieved their nuclear materials from Eastern Europe and the Baltics, as well as from submarines, but many remained closer to home, primarily in Georgia, Ukraine, Belarus, and Kazakhstan. Eventually, and after much diplomatic wrangling, these new nations agreed to the Nuclear Non-Proliferation Treaty and either destroyed the missiles and warheads on their soil or returned them to Russia, though stockpiles of plutonium and weapons-grade uranium remained behind. Security surrounding these materials, and at nuclear power plants, was often lax, raising fears that they could fall into the wrong hands. Within Russia, a poor economy, crime, and corruption raised fears of "loose nukes," or poorly guarded nuclear materials that could be stolen or sold to rogue states such as Iraq or Libya or to terrorist organizations, primarily al-Qaeda. The United States estimates that only about 40 percent of Russia's nuclear storage sites are up to U.S. security standards.

The U.S. response. Recognizing the need for the United States to provide assistance, Senators Sam Nunn of Georgia and Richard Lugar of Indiana sponsored legislation that allocated funds to help Russia and other former Soviet states either dismantle or secure nuclear materials. Congress agreed, and in 1991– 92 it authorized $800 million for the Nunn-Lugar Cooperative Threat Reduction Program. Each year after that, additional funds were authorized so that by 2001 the United States had provided $4 billion. These funds have been used by the Department of Defense (DOD), the Department of Energy (DOE), and other U.S. agencies to help the Soviet states destroy nuclear materials, upgrade security, and provide alternative employment for former Soviet nuclear scientists.

Nunn-Lugar funds have helped Russia, for example, deactivate nearly 5,800 nuclear warheads, destroy 439 ballistic missiles, eliminate hundreds of missile launchers and bomber aircraft, and secure nuclear materials by upgrading fencing, motion sensors, storage and transportation facilities, and the like. Originally, the George W. Bush administration had planned to cut funding for the program, but in the wake of the terrorist attacks on September 11, 2001, 2003 budget proposals called for $800 million for Russia, a 17 percent increase from 2002. Financial help is coming from other sources, too. At a 2002 summit, the industrialized nations pledged an additional $10 billion over the next ten years to help Russia eliminate or secure its nuclear arsenal, as well as its chemical and biological weapons.

The threat of "loose nukes." The true extent of the threat of "loose nukes" is uncertain and may never be known conclusively. Because of poor documentation at Russian nuclear storage sites, for example, materials could disappear, and it is plausible that no one in authority would know their status. Analysts thought that the problem was easing in the mid-1990s, but in the late 1990s and into the new century, instances of black-market smuggling seemed to be on the increase. Since 1993, the International Atomic Energy Agency (IAEA) in Vienna, Austria, a watchdog agency of the United Nations, has reported 411 cases of trafficking in nuclear materials. While 18 cases involved plutonium or weapons-grade uranium, most cases involved low-level medical and industrial radioactive waste, the kind used in dirty bombs. The first documented case of stolen Russian nuclear materials occurred in 1992, when an engineer at a nuclear research facility near Moscow stole three pounds of weapons-grade uranium. Fortunately, the case was resolved in almost comic fashion when the engineer was accidentally swept up in an arrest of a group of his neighbors suspected of theft from their workplace, and the uranium was discovered. Other cases have been more chilling. In 1994, Czech authorities searched a car parked on a street in Prague and discovered 3 kilograms of enriched uranium that came from an engineering institute near Moscow. Since 1999, three similar cases have been reported in Paris and Germany and at the Bulgarian-Romanian border.

An open question concerns the likelihood that an actual weapon could be stolen. The former Soviet states, including Russia, insist that no weapons have been stolen or reported missing, despite numerous efforts on the part

of terrorists and others to get their hands on one. Russian officials say that they have been vigilant in breaking up hundreds of plots to steal and smuggle nuclear materials and weapons, but U.S. officials believe that al-Qaeda and rogue states are always in the market for a nuclear bomb and could eventually succeed in getting one. More frightening is the prospect that poorly paid or unemployed Russian nuclear scientists might be vulnerable to the temptation to sell their know-how to terrorists or rogue states. The Japanese doomsday cult Aum Shinrikyo and the Taliban regime in Afghanistan tried, without success, to recruit Russian nuclear scientists.

Most troublesome is the possibility that so-called suitcase bombs—miniature nuclear devices weighing less than a hundred pounds and small enough to fit into a small container—have gone missing from Russia. These bombs could easily be smuggled into the United States or other countries, where they would cause enormous death and destruction. Indeed, in 1997 a former Russian general made headlines when he claimed that several dozen such Soviet-made bombs dating to the 1970s were unaccounted for. While Russian authorities insist that no such bombs ever existed, many Western analysts remain skeptical. Even if suitcase bombs never existed, the threat remains that small tactical nuclear weapons could be stolen or sold. These weapons pose a high threat for two reasons besides the relative ease with which they could be transported and hidden: one, they may lack safeguards that would prevent unauthorized detonation; and two, they have never been subject to arms-control treaty monitoring and verification, so their locations and the security surrounding them are difficult to assess.

FURTHER READING:

BOOKS:

Bunn, Matthew, Oleg Bukharin, and Kenneth N. Luongo. *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union.* Princeton, N.J.: Russian American Nuclear Security Advisory Council, 2000.

Marples, David R., and Marilyn J. Young, eds. *Nuclear Energy and Security in the Former Soviet Union.* Boulder, Colo.: Westview, 1997.

PERIODICALS:

Daughtry, Emily Ewell, and Fred L. Wehling. "Cooperative Efforts to Secure Fissile Material in the NIS." *Nonproliferation Review* 7, Spring 2000.

ELECTRONIC:

Council on Foreign Relations. "Loose Nukes," 2003. <http://www.terrorismanswers.com/weapons/loosenukes_print.html> (February 28, 2003).

Jasinski, Michael. "Nonproliferation Assistance to Russia and the New Independent States." Center for Nonproliferation Studies for the Nuclear Threat Initiative, August 2002. <http://www.nti.org/e_research/e3_4b.html>. (February 28, 2003).

Woolf, Amy F. "Nuclear Weapons in the Former Soviet Union: Location, Command, and Control." Congressional Research Service Report 91144, November 27, 1996. <http://www.fas.org/spp/starwars/crs/91–144.htm> (February 28, 2003).

SEE ALSO

Arms Control, United States Bureau
Ballistic Missiles
Cold War (1972–1989): The Collapse of the Soviet Union
Department of State, United States
DoD (United States Department of Defense)
DoE (United States Department of Energy)
International Atomic Energy Agency (IAEA)
Nonproliferation and National Security, United States

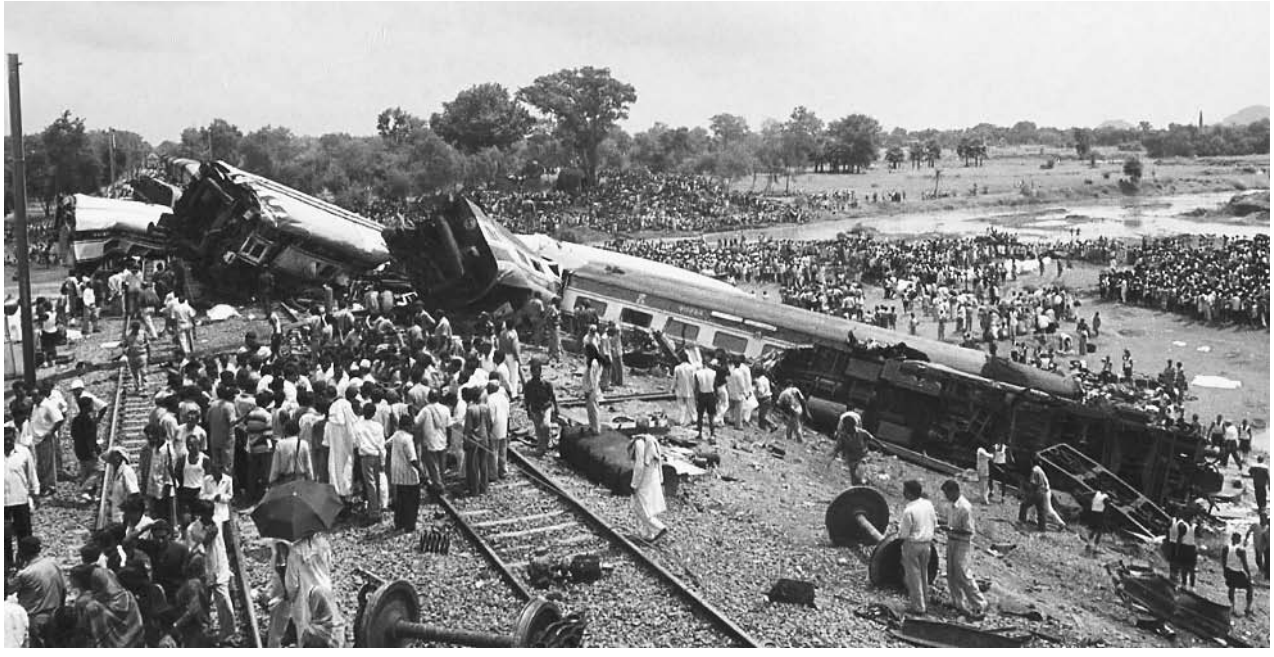
This page intentionally left blank

S

Sabotage

Sabotage is a deliberate act of destruction or work stoppage intended to undermine the activities of a larger entity, whether it is a business, government, or some other organization. The practice of sabotage, which has roots in the labor movements of the late nineteenth and early twentieth centuries, gained military and political application during the world wars and thereafter. It has also been a part of covert operations, often undertaken by agents provocateur.

There were isolated examples in earlier times, but probably the first case of organized—albeit apparently spontaneous—sabotage involved the Luddites of late eighteenth century England. Confronted by nascent industrialization and eager to hold on to their jobs, the Luddites destroyed labor-saving machinery. In 1910, striking French railway workers destroyed wooden railway ties or shoes, known as *sabots,* and from this act the word was coined. Ironically, a concept associated with labor movements was also used against organized labor by factory owners who hired agents provocateurs, infiltrators whose aim was to incite the local union to acts that would attract the attention of police.



Sabotage is suspected in the September 2002 derailment of an express train on its way from Calcutta to New Delhi in the Indian state of Bihar, leaving one car plunged into a river and two others dangling from a bridge. Fifty people died and 180 were injured. AP/WIDE WORLD PHOTOS.

In World War I, the Germans allowed Bolshevik leader V. I. Lenin to enter Russia through their territory, their intention being to sabotage the Russian leadership and pull the country out of the war—a gambit that succeeded. Although the Axis powers attempted to use sabotage against the United States, the most successful act of sabotage in World War II was the British and Norwegian effort to destroy the Germans' supply of heavy water, thus dashing Hitler's plans to build an atomic bomb.

During the postwar era, anticolonial movements in what came to be known as the developing world often used sabotage to remove Western influence. These acts ranged from the passive resistance to British rule by Indians under the leadership of Mohandas K. Gandhi, to the destruction of railway lines by revolutionaries fighting against the Portuguese in Angola and Mozambique. Communist-backed groups often used sabotage, although in Communist countries, any hint of real or imagined sabotage directed against the ruling system met with swift and severe punishment.

FURTHER READING:

BOOKS:

Bailey, Brian J. *The Luddite Rebellion.* New York: New York University Press, 1998.

Gallagher, Thomas Michael. *Assault in Norway: Sabotaging the Nazi Nuclear Bomb.* New York: Harcourt Brace Jovanovich, 1975.

Julitte, Pierre. *Block 26: Sabotage at Buchenwald.* Garden City, NY: Doubleday, 1971.

Sayers, Michael, and Albert Eugene Kahn. *Sabotage! The Secret War against America.* New York: Harper & Brothers, 1942.

Witcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914–1917.* Chapel Hill, NC: Algonquin Books, 1989.

SEE ALSO

Intelligence Agent
Soviet Union (USSR), Intelligence and Security

Salafist Group for Call and Combat (GSPC)

The Salafist Group for Call and Combat (GSPC) splinter faction that began in 1996 has eclipsed the *Groupe Islamique Armé* (GIA or Armed Islamic Group). since approximately 1998, and currently is assessed to be the most effective remaining armed group inside Algeria. In contrast to the GIA, the GSPC has gained popular support through its pledge to avoid civilian attacks inside Algeria (although, in fact, civilians have been attacked). Its adherents abroad appear to have largely co-opted the external networks of the GIA, active particularly throughout Europe, Africa, and the Middle East .

Organization activities. The GSPC continues to conduct operations aimed at government and military targets, primarily in rural areas. Such operations include false roadblocks and attacks against convoys transporting military, police, or other government personnel. According to press reporting, some GSPC members in Europe maintain contacts with other North African extremists sympathetic to al-Qaeda, a number of whom were implicated in terrorist plots during 2001.

Estimated organization strength and areas of operation. Although exact number are not known, intelligence analysts estimate that there are probably several hundred to several thousand GIA members operating inside Algeria .

GIA is supported by Algerian expatriates and GSPC members abroad, many residing in Western Europe, who provide financial and logistics support. In addition, the Algerian Government has previously accused Iran and Sudan of support of Algerian extremists.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Salmonella and Salmonella Food Poisoning

BRIAN HOYLE

Salmonella is the name of a group, or genus, of bacteria that live in the intestinal tract of warm-blooded animals,

including humans, as well as in cold-blooded animals such as turtles. The name of the microbe comes from its discoverer. In 1885, American veterinary scientist Daniel Salmon isolated the first strain (*Salmonella cholerasuis*) from the intestine of a pig.

Since his discovery, more than 2,300 different types of Salmonella have been discovered. While many of these can be innocuous in their normal intestinal environment, if they infect another area of the body (i.e., a cut) or contaminate food, illness can result.

Salmonella food poisoning, salmonellosis, affects two to four million Americans each year. The number of cases has been increasing in recent years, due in part to the increasing resistance of Salmonella to the antibiotics commonly used to treat the illness. It has been estimated by the Centers for Disease Control and Prevention that the economic cost of Salmonella food poisoning in the U.S. alone is between five and 17 billion dollars annually.

This economic burden, increasing prevalence of Salmonella food-borne illness, and the ease by which disease-causing strains of Salmonella could be acquired and deliberately added to food supplies, have made Salmonella one of the microorganisms that is regarded as being a potential threat to national security.

Salmonella food poisoning results from the growth of the bacterium in food. The rapid increase in the number of bacteria in the intestinal tract overwhelms the defensive capabilities of the host and produces the symptoms of food poisoning. Symptoms include nausea, vomiting, abdominal cramps, diarrhea, fever, and headache. Typically, the symptoms last for a few days.

Prolonged diarrhea can be dangerous. The body loses more fluids and salts than can be replaced, which can threaten the health of various organs and tissues in the body. In severe cases, especially in the young and the elderly, the resulting shock can cause permanent damage. As well, Salmonella can spread from the intestinal tract to the bloodstream, leading to more widespread infections.

The food poisoning caused by Salmonella is one of about ten bacterial causes of food poisoning. Other responsible bacteria include *Staphylococcus aureus*, *Clostridium perfringens*, *Vibrio parahaemolyticus*, and specific strains of *Escherichia coli*.

A number of foods are especially susceptible to contamination. Chicken carcasses and the outer surface of eggs are frequently contaminated with Salmonella present in the poultry feces. However, proper cooking will destroy the bacteria. The bacteria can gain entry to eggs through cracks in the shell. If the egg or meat is prepared at too low a temperature, the bacteria can survive and can multiply during subsequent storage at room temperature, or even at refrigeration temperature. Other targets for contamination include cream-based desserts, milk and dairy products, shrimp, salad dressing, cocoa, chocolate, and salad-type sandwich filling (such as tuna salad or chicken salad).

An important route of contamination is the handling of food by people who have not washed their hands properly after using the bathroom. This "fecal to oral" route of transmission can be prevented by hand washing, and proper kitchen hygiene (e.g., cleaning cutting boards after cutting raw poultry, storage of prepared foods in the refrigerator).

The thousands of different strains of Salmonella are also known as serotypes. These designations indicate that the differences between the strains lie mainly in the chemically different composition of the outer surface of the bacteria. The differences elicit different immune responses. The immune response for a particular strain is characteristic and can be useful in identifying the strain of Salmonella that is causing the malady. *Salmonella enteriditis* is of particular concern in food poisoning. This strain causes gastroenteritis and other maladies.

Strains like *Salmonella enteriditis* can establish infection because they have components that contribute to the infection. These components are classified as virulence factors. One of these factors is called adhesin. An adhesin functions in adhesion of the bacterium to a receptor on the surface of a host cell. An example of an adhesin is the tube-like structures called fimbriae that stick out from the surface of the cell.

Another virulence factor is lipopolysaccharide (LPS for short). LPS can help shield the surface of the bacterium from host antibacterial compounds. A part of the LPS called lipid A can cause a fever and a subcomponent of lipid A called endotoxin is harmful to the host. Salmonella also produces other toxins (e.g., enterotoxin). Because these toxins remain inside the bacterial cell, the increased number of bacteria that results from multiplication in the contaminated food increases the amount of the toxin ingested, and so increases the severity of symptoms.

The identification of Salmonella is not particularly difficult. Well-known lab media of defined composition exist, on which the bacteria grow and produce characteristic colours. For example, Salmonella grows on bismuth sulfide media and produces jet-black colonies, due to the production of hydrogen sulfide.

Unfortunately, however, the accurate diagnosis of Salmonella food poisoning usually comes after the fact, if the illness is diagnosed at all.

A vaccine that blocks the adhesion of the bacteria to the intestinal epithelial cells, which is a crucial part of the infection, could conceivably be developed. However, even if such a vaccine is possible, other vaccine needs that are more pressing currently occupy dedicated research resources. For the foreseeable future, the best strategy in preventing Salmonella food poisoning will remain the cooking of foods such as meat to the proper temperature for a recommended time, the proper storage of prepared foods, and good hygiene.

FURTHER READING:

BOOKS:

Fox, Nicols. *Spoiled: Why Our Food Is Making Us Sick and What We Can Do about It.* New York: Penguin USA 1998.

Salyers, Abigail, A., and Dixie D. Whitt. *Bacterial Pathogenesis: A Molecular Approach.* Washington, DC: American Society for Microbiology Press, 2001.

ELECTRONIC:

Centers for Disease Control and Prevention. "Salmonella Enteritidis." Division of Bacterial and Mycotic Diseases. April 25, 2001. <http://www.cdc.gov/ncidod/dbmd/diseaseinfo/salment_g.htm>(08 March 2003).

United States Food and Drug Administration. "Salmonella spp." Center for Food Safety and Applied Nutrition. January 10, 2003. <http://vm.cfsan.fda.gov/~mow/chap1.html>(02 March 2003).

SEE ALSO

Bioterrorism
Food supply, Counter-Terrorism
Infectious disease, threats to security
Pathogens

Sandia National Laboratories

K. LEE LERNER

Founded in 1949, Sandia National Laboratories, located in New Mexico (with additional laboratory facilities in California and Hawaii), is a government-owned facility managed by Lockheed Martin corporation for the Department of Energy (DOE). Sandia was originally managed by AT&T, but in 1993 Lockheed Martin assumed managerial control.

Sandia scientists and engineers participate in projects and programs designed to ensure the safety of the U.S. nuclear stockpile and maintain a high level of reliability in aging weapons. Increasingly key to safeguarding the nuclear stockpile is the development of high-speed virtual simulation capabilities that are able to model the complexities of the changes in weapons material as a function of time. Sandia programs also support the development of technologies and protocols that facilitate nonproliferation and secure control of nuclear materials (e.g., enhance weapon and surveillance technologies). Specific programs to enhance offsite monitoring include the advancement of robotics systems capable of monitoring proliferation activities.

Sandia supports programs seeking to assist Russia to safely manage and control nuclear materials from dismantled Soviet-era weapons systems.

Other less direct, but equally emphasized programs, are designed to enhance U.S. national security by developing technologies to protect critical infrastructure—especially energy production and delivery infrastructure. A specific aim of current Sandia projects involves potential integration of pulsed power technologies into defense-related applications. Other programs related to infrastructure protection are dedicated to extending the protection levels of radiation-hardened microelectronics.

In an effort to combat emerging threats, Sandia scientists and engineers are tasked with anticipating the need for new defense options and for developing technology capable of identifying (and neutralizing) biological and chemical agents. One Sandia innovation, "Amazing foam," is a nonhazardous decontaminating foam capable of rapidly neutralizing both chemical and biological agents.

Another Sandia innovation, the "magic cube," is capable of shaping a blast that blows a fragment-free hole in steel. Such developments have broad application. Magic cubes can be used to enhance low-invasive inspection of steel encased materials or to blow a hole in steel beams obstructing rescuers attempting to search through rubble or reach victims of a building collapse.

Sandia also devotes research resources to advancing techniques involved with hazardous material clean-up and the safe decommissioning and dismantling of obsolete weapons. Scientists at Sandia National Laboratories California collaborated with researchers at Lawrence Berkeley National Laboratory and Lawrence Livermore National Laboratory on the development of environmental remediation technologies useful in the cleanup of military disposal sites (e.g., the nearby Alameda Naval Air Station).

Sandia's technology transfer programs (where facets of defense related research are released and shared with private industry) are designed to increase United States' global economic competitiveness. The transfer is a bilateral arrangement that also allows industry input in defense design schemes. Other public programs sponsored by Sandia include educational outreach programs designed to foster excellence in scientific curricula and teaching.

Sandia scientists and engineers are highly involved in nuclear weapons production. Sandia designs and engineering integration impact and more than 6,300 parts of the estimated 6,500 components of modern nuclear weapons. Other programs designed to enhance national security includse highly specialized and sophisticated modeling and testing facilities that allow Sandia scientists to test updates to weapons systems without actual nuclear testing. Failsafe technologies—devoted to preventing accidental nuclear detonation—include sophisticated arming and firing systems (e.g., the MC2912 arming system utilized on the W76/Mk4 nuclear warhead).

Sandia's sensory technology programs are designed to detect nuclear materials as well as chemical and biological weapons agents.

Scientists at LBL, Lawrence Livermore National Laboratory (LLNL), and Sandia National Laboratories California have also collaborated on the development of environmental remediation technologies useful in the cleanup of

A Sandia National Laboratories researcher speaks by phone with someone inside an early model of the ultra-clean room invented in 1962. Sandia is also responsible for about 98 percent of the 6,000 non-nuclear parts in nuclear weapons. AP/WIDE WORLD PHOTOS.

military disposal sites (e.g., the nearby Alameda Naval Air Station).

In April 2003, Sandia scientists reported that they had achieved controlled thermonuclear fusion in a pulsed power source. If ultimately reproduced and verified, the process, and other competing approaches to controlled fusion, holds the promise of nearly unlimited clean power generation. Unlike fission reactions, fusion based energy technology would not produce long-lived radioactive waste.

Instead of using magnetic containment to compress hydrogen and thereby achieve temperatures hot enough for fusion to occur, Sandia scientists used pulsed releases of current to achieve a rapid series of limited micro fusion reactions. Using an improved and more powerful Z accelerator, high current is induced in a tungsten wire cage surrounding a 2 mm plastic capsule containing deuterium (a heavier isotope of hydrogen). The tungsten cage is vaporized, but the short-lived current impulse generated in the wires creates a powerful magnetic pulse and shockwave of superheated tungsten that creates an intense x-ray source that, along with the shockwave compresses and heats the hydrogen to more than 20 million degrees Fahrenheit (more than 11 million degrees Celsius) to induce fusion.

The Sandia reaction process contrasts with another promising approach undertaken at the Lawrence Livermore National Laboratory (LLNL) that seeks to initiate fusion reactions by shining high-energy lasers on hydrogen globules. The LLNL approach will be further explored at the National Ignition Facility.

FURTHER READING:

ELECTRONIC:

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm> (March 23, 2003).

United States Department of Homeland Security. Research & Technology. <http://www.dhs.gov/dhspublic/display?theme=27&content=374> (March 23, 2003).

SEE ALSO

Argonne National Laboratory
Brookhaven National Laboratory
DOE (United States Department of Energy)
Environmental Measurements Laboratory
Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory (LLNL)
Los Alamos National Laboratory
NNSA (United States National Nuclear Security Administration)
Oak Ridge National Laboratory (ORNL)
Pacific Northwest National Laboratory
Plum Island Animal Disease Center

Sarin Gas

JULI BERWALD

Sarin gas (O-Isopropyl methylphosphonofluoridate), also called GB, is one of the most dangerous and toxic chemicals known. It belongs to a class of chemical weapons known as nerve agents, all of which are organophosphates. The G nerve agents, including tabun, sarin and soman, are all extremely toxic, but not very persistent in the environment. Pure sarin is a colorless and odorless gas, and since it is extremely volatile, and can spread quickly through the air. A lethal dose of sarin is about 0.5 milligrams; it is approximately 500 times more deadly than cyanide.

History and global production of sarin. Sarin was first synthesized in 1938 by a group of German scientists researching new pesticides. Its name is derived from the names of the chemists involved in its creation: Schrader, Ambros, Rudriger, and van der Linde. A pilot plant to study the use of sarin was built in Dyernfurth. Although they produced between 500 kg and 10 tons of sarin, the German government decided not to use chemical weapons in artillery during World War II. The Soviet army captured the plant at Dyernfurth at the end of the war and resumed production of sarin in 1946. The Russian government currently has about 11,700 tons of sarin.

Between about 1950 and 1956, the United States produced sarin. It is estimated to have stockpiles totaling 5,000 tons of the nerve agent stored in different parts of the country. Several other countries including Syria, Egypt,

Subway passengers affected by sarin gas planted in central Tokyo subways are carried to the hospital in March 1995. Years after the Aum Shinri cult's terrorist attack in which 11 people were killed and thousands were injured, many victims still suffer physical symptoms from the gas. AP/WIDE WORLD PHOTOS.

Iran, Libya, North Korea, and Iraq have confirmed or suspects stocks of sarin.

Sarin as a weapon. Iraq produced sarin between 1984 and 1985, when weapons inspectors were ordered to leave the country. Prior to Operation Iraqi Freedom, Iraq had admitted to once having at least 790 tons of the nerve agent. In 1987 and 1988, the United Nations confirmed that Iraq used a combination of organo-phosphorous nerve agents against Kurds in northern Iraq. It is estimated that 5,000 people were killed and 65,000 others were wounded in these attacks. There was also extreme environmental damage.

On March 20, 1995, the Aum Shinrikyo doomsday cult released the nerve agent sarin in a Tokyo subway. This incident killed 11 and injured more than 5,500 people. Members of the cult left soft drink containers and lunch boxes filled with the toxin on the floor of subway trains. They punctured the containers with umbrellas just as they exited the cars. The attack was timed for rush hour, so as to affect as many people as possible. Because the sarin was of low quality and the affected cars were quickly sealed once the sarin was detected, the magnitude of the attack was suppressed.

Sarin poisoning. Like other organophosphate nerve agents, sarin inhibits the break down of the enzyme acetylcholinesterase. Under normal conditions, this enzyme hydrolyzes the neurotransmitter acetylcholine. When sarin is present, the build up of acetyl-cholinesterase results in the accumulation of excessive concentrations of acetylcholine in nerve synapses. This overstimulates parasympathetic nerves in the smooth muscle of the eyes, respiratory tract, gastrointestinal tract, sweat glands, cardiac muscles, and blood vessels.

After exposure to sarin, symptoms begin within minutes. If a person survives for a few hours after exposure, he or she will likely recover from the poisoning. The first symptoms of sarin poisoning include a runny nose, blurred vision, sweating, and muscle twitches. Longer exposures result in tightness of the chest, headache, cramps, nausea, vomiting, involuntary defecation and urination, convulsions, coma, and respiratory arrest.

Atropine acts an antidote for nerve agent, including sarin. Atropine binds to one type of acetylcholine receptor on the post-synaptic nerve. A second antidote is pralidoxime iodide (PAM), which blocks sarin from binding to any free acetyl-cholinesterase. Both should be administered as soon as possible following exposure to the toxin. Diazapam can also be used to prevent seizures and convulsions. Soldiers fighting in regions where chemical weapons are likely to be deployed are now equipped with a Mark I antidote kit containing both atropine and PAM.

FURTHER READING

ELECTRONIC:

Centers for Disease Control and Prevention: "Facts About Sarin" <http://www.bt.cdc.gov/agent/sarin/basics/facts.asp> (March 25, 2003).

Council on Foreign Relations: Terrorism Questions and Answers, "Sarin" <http://www.terrorismanswers.com/weapons/sarin.html> (March 25, 2003).

"Sarin Poisoning on Tokyo Subway" <http://www.sma.org/smj/97june3.htm> (March 25, 2003).

SEE ALSO

Biological Warfare
Nerve Gas
Toxins

SARS (Severe Acute Respiratory Syndrome).

SEE *Communicable Diseases, Isolation, and Quarantine.*

Satellite Technology Exports to the People's Republic of China (PRC)

JUDSON KNIGHT

The issue of satellite technology exports from the United States to the People's Republic of China (PRC) mirrored larger concerns over Chinese espionage that surfaced in the late 1990s. In the case of satellite technology sales, however, United States companies and even some sectors of the federal government favored at least some degree of technology transfer, if only to maintain good relations between the two countries. This was particularly the case after September 11, 2001, as President George W. Bush sought to establish stronger ties with the Chinese in the fight against terrorism. Still, questions remained regarding the advisability of some such transfers, as well as the legality of transfers that had taken place in the mid-1990s and later.

Allegations in the 1990s. During the administration of President William J. Clinton, a number of critics charged that the president had been involved in a scheme to channel funds from the PRC to the Democratic National Committee. Clinton's defenders dismissed the criticism as a partisan attack from the far Right, and while most of the

critics were conservatives, not all of them could be dismissed as extremists. An example was the respected columnist William Safire, who wrote in the *New York Times* on May 18, 1998, that "A president hungry for money to finance his re-election overruled the Pentagon; he sold to a Chinese military intelligence front the technology that defense experts argued would give Beijing the capacity to blind our spy satellites and launch a sneak attack." Complicit Democrats in the Senate, Safire and others charged, had blocked efforts to investigate the illegal transfer of technology.

One particular point of contention was the fact that Clinton had given the Department of Commerce increased jurisdiction over satellite technology transfers. This was significant in light of allegations that a Commerce official, John Huang, had ties to the Chinese. The sale of satellite communications technology to China had first been permitted by President Ronald Reagan, who in September 1988 negotiated a bilateral agreement with the PRC to ensure that no missile or satellite technology was transferred. Over the next four years, the State Department licensed all communications satellites, but as a result of a review conducted by the administration of President George Bush in 1990, licensing jurisdiction for purely commercial satellites was transferred to Commerce. Franklin C. Miller, Principal Assistant Secretary of Defense for Strategy and Threat Reduction, testified before the Senate Committee on Commerce, Science, and Transportation in September 1998, that Defense had supported this act because it "was accompanied by several changes in procedures that protect Department of Defense's ability to ensure that transfers are consistent with U.S. national security."

Despite this testimony, Henry Sokolski of the Nonproliferation Policy Education Center maintained that Clinton had gone much further than his predecessors. In testimony before a joint hearing of the House International Relations Committee and the House National Security Committee in June 1998, he maintained that "this shift has eliminated systematic government monitoring of prelaunch conversations between U.S. contractors and Chinese space firms and, according to the General Accounting Office, marginalized the previously important licensing input of the Defense Department." As though to underscore Sokolski's point, it was later revealed that in 1996, Loral Space & Communications Corporation had forwarded a report on a Chinese rocket to the Chinese government without first obtaining State Department clearance, a situation that led to a grand jury investigation.

A change of course in the 2000s. A concern similar to that involving Loral erupted in late 2002, when the State Department accused Hughes Electronic Corporation of providing the Chinese with key information to assist them in determining why their rockets tended to fail soon after launch. The incident had occurred in the 1990s, according to the State Department—in other words, at the high point of concerns over the transfer of sensitive satellite technology to the PRC. Although the State Department threatened fines of up to $60 million, by the time the charges came to light, the situation with regard to satellite technology transfers to the PRC had changed.

This change did not so much involve security as it did commerce—specifically, an increased demand by U.S. aerospace companies to relax restrictions on transfers. The change created some strange political bedfellows: joining fellow California representative Howard L. Berman, a Democrat, in putting forward the proposal was Dana Rohrbacher, a Republican who had opposed the Clinton-era transfer of licensing authority to Commerce. Yet, in 2001, Rohrbacher—whose constituency, like that of Berman, had a strong aerospace presence—supported the very measure he had condemned three years earlier. Just as Berman and Rohrbacher constituted a bipartisan team, they found themselves opposed from both sides of the aisle. Not only Republican senators Jesse Helms and Richard Shelby, but also Democratic representative Tom Lantos of California, maintained that the move posed security risks.

By that time, however, the tides had shifted, and the move to increase sales of satellite technology to China gained momentum. In April 2002 the State Department loosened rules on export of scientific satellite projects to the PRC. Six months later, as Chinese head of state Jiang Zemin met with President George W. Bush at the latter's ranch in Texas, the two discussed the possibility of easing bans on the transfer of satellite technology, provided China reduced its sales of missile technology to third parties. The leaders did not reach an agreement, however, and debate continued. On March 28, 2003, during the U.S. military effort against Iraq, a missile fired by the Iraqis hit a shopping mall in Kuwait, a country aligned with the United States in the war. The weapon was a modified Chinese-made Silkworm rocket.

FURTHER READING:

PERIODICALS:

Lawler, Andrew. "Rules Eased on Satellite Projects." *Science.* 296, no. 5566 (April 12, 2002): 237–238.

Marquand, Robert. "As War Looms, U.S. Talks to China." *Christian Science Monitor.* (October 21, 2002): 6.

Marquis, Christopher. "Some Lawmakers Urging U.S. to Speed Exports of Satellites." *New York Times.* (July 9, 2001): A7.

Safire, William. "China Syndrome: Clinton's Greed for Funds Triggers a Security Meltdown." *New York Times.* (May 18, 1998): A19.

ELECTRONIC:

Defense DAS Miller on Technology Transfers to China. U.S. Department of State. <http://usinfo.state.gov/regional/ea/uschina/millr917.htm> (March 29, 2003).

Sokolski, Henry. U.S. Satellite Technology Transfers to China: What's at Issue, Questions and Answers. Nonproliferation Policy Education Center. <http://www.npec-web.org/presentations/sat_trans.htm> (March 29, 2003).

SEE ALSO

Chinese Espionage against the United States
Satellites, Non-Governmental High Resolution
Satellites, Spy

Satellites, Non-Governmental High Resolution

WILLIAM C. HANEBERG

Satellite imagery at resolutions useful for military and intelligence purposes has historically been available only from satellites developed, launched, and operated by governments. As a result, access to and dissemination of the high-resolution satellite images was tightly controlled in the interest of national security. Since 1999, however, commercial satellites have made high-resolution images publicly available at a relatively low cost. In the United States, the Land Remote Sensing Policy Act of 1992, which was motivated in part by Russian willingness to sell declassified 2 m resolution military satellite imagery in the early 1990s, provided the legal foundation for private ownership of American remote sensing satellites. In 1994, the Clinton administration issued guidelines for the licensing of commercial remote sensing satellite operations.

The resolution of an image is the size of the smallest object that can be depicted, and the best images currently available from commercial satellites have resolutions ranging from 50 cm to 1 m. Imagery from the most recent intelligence satellites launched by the United States government, in contrast, is believed to have a resolution of about 2 cm. No images with this resolution, however, have been released to the public. Although there is no universally accepted definition of "high resolution," in part because its meaning changes as technology improves, at the time this article was written it was generally understood to mean resolutions of 2 m or less.

IKONOS, named after the Greek word for "image," was the first commercial satellite to provide images with 1 m resolution. Its products include 1 m panchromatic (black and white) and true color images in addition to 4 m multispectral imagery. Following a sun-synchronous orbit 680 km above Earth's surface, IKONOS passes over any given longitude at about 10:30 a.m. local time each day and revisits any given geographic location every three days. Space Imaging, the company that operates IKONOS was founded by a consortium of firms from the United States, Japan, and South Korea. The satellite was launched in August 1999 after the first version was destroyed when its launch vehicle malfunctioned and crashed the previous spring.

A satellite image showing the Yongbyon nuclear facility in North Korea taken in 2002. According to the Institute for Science and International Security (ISIS), significant facilities in the image include a five-megawatt reactor and cooling tower, and a spent fuel storage building in the bottom of the site near the river. AP/WIDE WORLD PHOTOS.

Developed by an international consortium of companies based in Cyprus and known as ImageSat International (ISI), the EROS A1 satellite was built largely in Israel and launched in 2001 from a Russian facility in Siberia. It was the first high-resolution commercial satellite developed outside of the United States. The EROS A1 camera, which can provide 1.8 m resolution panchromatic images, is

A view of the port and downtown areas of Abu Dhabi made by the QuickBird satellite provided by DigitalGlobe. QuickBird snaps some of the most detailed satellite images available to the public. AP/WIDE WORLD PHOTOS.

based on technology originally developed for Israeli intelligence satellites. The successor the EROS A1, known as the EROS B1, is scheduled for launch in late 2004 and is expected to produce both panchromatic and multi-spectral color imagery with 0.87 m resolution.

The highest resolution commercial imaging satellite currently in operation is QuickBird, operated by the Colorado-based firm Digital Globe, which follows a sun-synchronous orbit 450 km above Earth. The first QuickBird was lost in space after a late 2000 launch from a Russian facility in Siberia. A replacement was successfully launched from Vandenberg Air Force Base, California, atop a Delta II launch vehicle in late 2001. QuickBird supplies 0.62 m resolution panchromatic images and 2.4 resolution multispectral color images.

Proponents of commercial high-resolution imaging satellites argue that their images will be useful for a variety of civil work that includes infrastructure monitoring, natural disaster recovery, endangered species habitat identification and monitoring, and natural resource exploration. Commercially available high-resolution images can also be used to monitor troop and equipment movement,

observe construction activity, identify targets in inaccessible areas, and remotely assess battle damage. This has led the United States government to prohibit its licensees from obtaining or selling high-resolution imagery of Israeli territory in response to concerns raised by the government of Israel. It also reserves the right to restrict operations during times of national security emergencies. These restrictions do not apply, however, to commercial satellites operated by companies outside of the United States.

Israel launched the Ofek-5 spy satellite at a coastal air force base south of Tel Aviv in 2002 to exted its ability to monitor developments in the region. AP/WIDE WORLD PHOTOS.

■ FURTHER READING:

BOOKS:

Bossler, John D., John R. Jensen, Chris McMaster, and Chris Rizos (editors). *Manual of Geospatial Science and Technology.* Mount Laurel, New Jersey: Taylor & Francis, 2001.

Campbell, James B. *Introduction to Remote Sensing (3d edition).* New York: Guilford Press, 2002.

ELECTRONIC:

Baker, J.C. "Commercial Observation Satellites: A Catalyst for Global Transparency." 2002. <http://www.imagingnotes.com/julaug01/global.htm> (12 April 2003).

"Digital Globe." <http://www.digitalglobe.com/> (12 April 2003).

"ImageSat International." 2003. <http://www.imagesatintl.com/> (12 April 2003).

"Space Imaging—Visual Products. Visible Results." 2003. <http://www.spaceimaging.com/>(12 April 2003).

SEE ALSO

Cameras
Geospatial Imagery
LIDAR (Light Detection and Ranging)
Photographic Resolution
Photography, High-Altitude
Remote Sensing

Satellites, Spy

■ LARRY GILMAN

Spy satellites are robotic observational platforms that orbit the Earth in order to image its surface and to record radio signals for military and political purposes. They transmit their data to Earth, where it is interpreted by specialists in centralized, secretive facilities such as the U.S. National Photographic Interpretation Center in Washington, D.C. Spy satellites have been essential not only to military operations and the formation of national policy but to the verification of arms control treaties such as SALT I, SALT II, and the Comprehensive Test Ban Treaty.

Hundreds of spy satellites have been launched since 1960, when the U.S. lofted its first. The four basic types of spy satellite are: (1) photoreconnaissance systems that take pictures in visible and infrared light, (2) infrared telescopes designed to detect missile launches, (3) radars that image sea or land even through cloud cover and in darkness, and (4) signals intelligence (SIGINT) satellites (also termed "ferrets"), which are optimized either for characterizing ground-based radar systems or for eavesdropping on communications. Sometimes photoreconnaissance and SIGINT functions are combined in single, massive platforms such as the U.S. Keyhole-series satellites.

Although a number of nations have launched spy satellites, the U.S. and the Soviet Union are responsible for by far the greatest number. The Russian Federation, which inherited most of the Soviet Union's space system after 1991, has been unable to afford the cost of adequately updating its spy satellite network. In contrast, the U.S. has continued to deploy ever-more-sophisticated systems in a steady stream. Thus, the majority of spy satellites in orbit today, including all the most capable units, are U.S.-owned. Although the precise technical capabilities (and in many cases even the basic missions and orbits) of U.S. spy satellites are secret, it is thought that the best U.S. visible-light spy satellites are capable, given

clear skies, of imaging surface features only a few centimeters across. A modern U.S. spy satellite can, given clear skies and a good viewing angle, probably read a license plate from space.

Early U.S. Spy Satellites: Corona, MIDAS, SAMOS

The U.S. began developing spy satellites in the mid-1950s, years before it had a rocket capable of placing anything in orbit. As early as 1946, RAND (short for the RAND or *R*esearch *an*d *D*evelopment Corporations, a think tank created by Douglas Aircraft Co. that was influential throughout the Cold War) had produced a report entitled "Preliminary Design of an Experimental World-Circling Spaceship." The usefulness of such systems was obvious long before they were buildable, for military forces had been seeking higher vantage points from which to observe the enemy ever since the U.S. Civil War, when the Union experimented with tethered observation balloons overlooking Confederate positions. In the early twentieth century, reconnaissance blossomed when photographic film replaced cumbersome glass plates and cameras were borne aloft on aircraft. So effective is aerial photography that it is still used today; the U.S., for example, continues to employ its high-altitude U-2 and SR-71 Blackbird aircraft, early versions of which it developed in the 1950s and 1960s.

However, spy planes have limitations. Even the highest-flying airplane cannot fly above the atmosphere, and can therefore, view only a limited amount of ground at any one time. Even at four times the speed of sound (the approximate top speed of an SR-71), this is a severe disadvantage when trying to surveil a country as large as China or Russia. Nor can planes be kept aloft indefinitely; they must be sent out at intervals. They must also be piloted, putting crew members at risk of death or capture. This was illustrated most famously in 1960, when CIA pilot Gary Powers was shot down while flying a U-2 spy plane over the Soviet Union and tried for espionage. (In recent years, robotic aircraft have been employed for some short-range aerial reconnaissance.) Finally, spy planes are intrinsically illegal in time of peace—they must violate national airspace to do their job—and therefore, a political liability.

Spy satellites overcome all the limitations of spy planes. A network of three geosynchronous satellites can, in contrast to the occasional glimpses provided by spy planes, keep the entire world in view at all times. (A geosynchronous satellite orbits 22,160 mi [35,663 km] above the equator in the direction of the Earth's rotation, matching its movement with the Earth's surface so that it appears to hover at a fixed point in the sky.) A network of lower-altitude satellites in polar orbits (i.e., circling at right angles to the equator, over the poles) can, by combining their smaller fields of view, do the same. Also, satellites are at an altitude too high to be easily shot down, though the U.S. and Russia have developed anti-satellite weapons in case they should ever wish to do so. Finally, satellites are legal: they do not violate national airspace. This legal point was not always universally acknowledged; for a few months in 1960 the Soviet Union complained that U.S. spy satellites were violating its airspace, which, it said, extended upward indefinitely from its territory. It dropped this argument when it began launching its own spy satellites in October, several months after the United States.

The U.S. Air Force and Central Intelligence Agency (CIA) were early advocates of satellite surveillance. ("Surveillance," strictly speaking, refers to the passive, ongoing observation of some area to scan for activities or changes of interest, while "reconnaissance" refers to the active seeking of specific information at a particular time; however, the word "surveillance" is often used to cover both activities.) A detailed study released by RAND in 1954 suggested two basic methods for returning imagery to Earth from an orbiting platform: (1) television pictures scanned from photographic film on board a spacecraft and beamed to Earth, and (2) return of the film itself to Earth in a reentry vehicle. The Air Force decided to develop the first option, arguing that retrieving film from space would be time-consuming and unreliable; the CIA decided to develop the second, reasoning that TV technology was still too crude to give sufficiently high-resolution pictures.

Squabbling between the Air Force and CIA, both jockeying for control of U.S. space surveillance resources, eventually moved President Dwight Eisenhower to create the National Reconnaissance Office (NRO) on August 25, 1960. Then NRO (officially secret until the early 1990s) is staffed by personnel from the Air Force, CIA, and other government agencies and is charged with overseeing the United States's space-surveillance programs. Under the NRO's guidance, three major spy-satellite programs went ahead in the early 1960s, one directed by the CIA and two by the Air Force.

The CIA's system, code-named Corona, took high-resolution photographic negatives with orbiting telescopic cameras and then dropped them to the Earth. The first 12 attempts to achieve orbit or return film all failed, but starting with Corona 13 in August, 1960, Corona began to fulfill its promise. A long series of Corona satellites were launched, orbited over the Soviet Union, and returned their exposed film in reentry capsules. Each capsule deployed a parachute after it had killed most of its velocity by friction with the atmosphere, and was then hooked from the air by a propeller-driven JC-130B aircraft flying at about 150 miles per hour (242 km/hr). The Corona satellites returned excellent images, with later models probably achieving a resolution of about 1 foot (.3 m). One of Corona's first achievements was to debunk the Air Force's claims that a huge "missile gap" existed in the early 1960s between the Soviet Union and the U.S.—that is, that the

Soviets many more ICBMs (intercontinental ballistic missiles) than the U.S. In fact, as Corona showed, the Soviets actually had far fewer missiles than the U.S. at that time.

Because each Corona satellite had a limited film supply, it remained in orbit only for hours or a few days, requiring that a new Corona be launched each time a new set of photographs was desired. Corona, therefore, did not keep the Soviet Union under constant surveillance, but instead ran a series of reconnaissance missions with specific goals. Over 120 Corona satellites were flown before being replaced in the early 1970s by the larger and more sophisticated film-return satellite known as KH-9 HEXAGON (or "Big Bird").

The two spy-satellite programs pursued by the U.S. Air Force in the early 1960s were SAMOS (Satellite and Missile Observation System) and MIDAS (Missile Alarm Defense System). SAMOS satellites took pictures on film, developed the film in orbit, and transmitted TV scans of the pictures to Earth. Because the TV pictures were much blurrier than the film, SAMOS had low resolution even for its day (5–20 feet), and some authorities (e.g., Herbert Scoville, Jr. [1915–1985], arms-control expert and one-time CIA analyst) have claimed that SAMOS never produced useful data. It was not until the 1970s, with the launch of the KH-11 spy satellite (discussed further below), that radio return of data from orbit was to provide images as good as those available directly from film. The first successful SAMOS launch was on January 31, 1961; 26 more SAMOS satellites were launched between then and November 27, 1963, when the program ended.

Meanwhile, the Soviet Union was launching its own series of low-orbit photoreconnaissance satellites, the Cosmos platforms. Like Corona, the Cosmos satellites were film-return missions—a technique that the Soviet Union (and, later, the Russian Federation) would continue to use until 2000, when the Enisei satellite, designed to return high-resolution digital images in real time like the United States's KH-11 and KH-12 satellites, was launched. The Cosmos were modified Vostok capsules originally designed to carry cosmonauts, rather than specialized platforms. (Later, the Soviets would also modify their larger Soyuz capsules for use as robotic spy satellites). Use of Vostok capsules had the advantage that the Soviets did not have to invent a separate film-return system, having already developed techniques for landing Vostok capsules by parachute.

Corona, SAMOS, and Cosmos followed polar orbits at altitudes of about 150 miles, circling Earth every 90 minutes or so. (Satellites at lower altitudes get a closer view but encounter atmospheric drag that shortens their lifetimes, eventually burning them up like meteors; spy satellites have been orbited as low as 76 miles, but they did not last long.) A polar-orbiting photoreconnaissance satellite views a limited portion of the surface at any one time, although its field of view moves rapidly over the Earth as the satellite speeds through space. MIDAS, the U.S. Air Force's other early spy-satellite project, was different. Each MIDAS satellite was stationed at a much altitudes (e.g., 2170 mi [3500 km]), from which it could see most or all of the Soviet Union at any moment. The MIDAS satellites were designed not to take visible-light images of the Earth, but to observe it in the infrared band of the electromagnetic spectrum. The goal was to detect the heat radiation (infrared light) given off by missile and rocket launches; MIDAS could radio warning of an attack to Earth long before ground-based radars could detect approaching missiles. Twelve attempts to orbit MIDAS satellites were made between February, 1960, and October, 1966. Most failed, but experience with MIDAS made possible its successor, the Defense Support Program (DSP) system of geosynchronous infrared early-warning satellites.

Defense Support Program

The first DSP early-warning satellite was launched in 1970, the nineteenth in 1999. Unlike their predecessors, the MIDAS satellites, DSP satellites are deployed to geosynchronous orbits. Five are usually in operation at any one time: the three newest are used to observe parts of the Earth deemed most likely to be missile launch sites (e.g., Russia), while the two oldest are used both to observe less-critical areas and as backups for the first three. When a new DSP satellite is launched, the most obsolete of the five already in orbit is nudged by its rockets to a higher orbit in order to avoid cluttering the geosynchronous altitude.

DSP satellites combine high resolution with wide-area coverage by a mechanical trick. The field-of-view of a DSP satellite's telescope is much smaller than the disk of the Earth, but the telescope is mounted at an slight angle to the long axis of the satellite, which is caused to spin at .175 revolutions per second. The working satellite thus resembles a rolling bottle with an off-angle straw protruding from its mouth, where the straw corresponds to the telescope and is pointed toward Earth. The telescope's field of view is wobbled systematically over a larger area of the Earth than it would view if the satellite were stationary.

The data collected by DSP satellites are compressed by on-board computers and then transmitted to a data-collection station at Nurrungar, Australia, where they are analyzed in real time. This system underwent an unplanned but crucial test in 1979, when a computer tape simulating an all-out Soviet nuclear attack was mistakenly fed into the early-warning system of the U.S. Strategic Air Command's control center in Colorado. Controllers assumed that a real attack was occurring, and U.S. ballistic-missile crews prepared to launch in retaliation. War was averted because U.S. leaders took the precautionary step of viewing real-time date from the DSP satellite system, which showed that no launches had actually occurred in the Soviet Union.

The Soviet Union, although always lagging the U.S. technologically, has also deployed infrared early-warning satellites. By the early 1990s, it had several "Prognoz" satellites in geosynchronous orbits doing the same job as the United States's DSP satellites. It also had a collection of nine "Oko" (Russian for "eye") satellites, also infrared

early-warning platforms, in elliptical (off-center) orbits. The latter were designed to observe the missile fields of the continental U.S. at a grazing angle. The advantage of such a view for early warning is that U.S. missiles would, within seconds of liftoff, be silhouetted against the blackness of space, making them easier to detect. Today, only one Prognoz early-warning infrared satellite remains operational. To decrease the likelihood of a Russian ballistic-missile launch due to flawed or inadequate information, some experts have proposed that the U.S. and Russia set up a joint early-warning center where the U.S. would share its DSP data with Russian observers.

Keyhole. Since March, 1962, all U.S. photographic intelligence satellites and aircraft have been managed under the program name "Keyhole." Keyhole satellite designs are given Keyhole numbers; SAMOS and Corona were retrospectively labeled KH-1 and KH-4. (There seems not to have been a KH-2 or KH-3.)

A dozen Keyhole satellite designs have been orbited to date, each generation containing a significant improvement over its predecessor. In the days when each satellite (whether a "bucket dropper"—film-return—type or TV-scanning type) carried a finite supply of photographic film, satellite lifespans were short and large numbers of each type were launched. For example, 46 copies of the KH-5 satellite (the immediate successor to the Air Force's SAMOS) were launched from 1963 to 1967. Thirty-six copies of Corona's successor, the KH-6, were orbited during the same period. The two satellite types were used in conjunction; low-resolution, wide-area images from a KH-5 would be used to identify targets for high-resolution, "close-look" reconnaissance by a KH-6.

The next close-look satellite, the KH-8 (still a bucket-dropper), was the first spy satellite to examine bands of the electromagnetic spectrum other than the visual-light band. Since the KH-8, all Keyhole satellites have examined light in several narrow bands in the visible and infrared parts of the spectrum. This is done in order to extract maximum information about ground features. A different lens must be used for each wavelength, as a single lens cannot focus all wavelengths simultaneously. This adds to the complexity and cost of each satellite, but increases its usefulness greatly.

The most famous Keyhole satellite type is the KH-11, the primary U.S. orbital imaging platform from 1976 to 1992 (when it was succeeded by the KH-12, still in service today). The KH-11 finally achieved the ambition of SAMOS's designers: to return film-quality images from orbit electronically, without bucket-dropping. The invention of the charge-coupled device (CCD) in 1970 was key to this advance, and has transformed astronomy as well. A CCD is a microchip (i.e., a thin rectangle consisting mostly of silicon or another semiconductor, >.5 in^2); one side of the chip is an array of thousands of microscopic electronic devices that record photon impacts as electrical charges. (A photon is the minimum unit of light.) Placing a CCD in the focal plane of a telescope and periodically reading off the contents of its array of photon sensors produces a digital image record. The CCD is thus the equivalent of the film in a conventional camera, with the difference that a CCD can be re-used indefinitely.

The image information from a CCD is stored in digital form. Digital information, unlike the analog TV signals from the original SAMOS, is easy to encrypt and to transmit without loss of quality. Furthermore, the abandonment of bucket-dropping meant that spy satellites could remain in orbit for years rather than weeks. This, in turn, has made it feasible to invest more money in each satellite, making it more complex and capable. (A modern KH satellite costs about a billion dollars.) SIGINT antennas were added to KH-11s as the series progressed, to eavesdrop on communications.

KH-11 and KH-12 satellites are also highly maneuverable. A KH-12 satellite carries some seven tons of hydrazine fuel with which to maintain its orbital altitude against atmospheric drag or to change its orbit in order to better view specific parts of the Earth.

SIGINT and ferrets. Signals intelligence (SIGINT) is divided into three sub-fields: communications intelligence (COMINT, the interception of messages), electronics intelligence (ELINT, the gathering of information about radar, radar jammers, and the like), and telemetry intelligence (TELINT).

TELINT is in fact a special type of COMINT. Telemetry is data about physical quantities measured by automatic devices, often embedded in missiles, spacecraft, or aircraft. When a new ballistic missile is tested, say by China, it radios a complex telemetry stream to the ground from the moment of its launch until it crashes or explodes. The telemetry stream is intended to show the missile's designers exactly how the new machine is performing and, if it fails, what components caused the failure. (As a famous unclassified example, analysis of routinely-recorded telemetry from the space shuttle *Columbia* was essential to understanding the causes of that spacecraft's explosion during reentry in 2003.) The telemetry—once decoded, a task accomplished by the U.S. National Security Agency (NSA) or a foreign equivalent—also reveals the detailed mechanics of the missile to TELINT eavesdroppers: fuel consumption, acceleration, guidance, and the like.

TELINT and COMINT collection are the primary missions of the U.S. Rhyolite series of satellites (also termed Aquacade), the first of which was launched in 1973. The Rhyolites are also thought to collect some ELINT (radar mapping data). Rhyolites must observe the Earth continuously in order to eavesdrop effectively on communications sessions, which usually last more than the few minutes that a fast-moving, low-altitude satellite is in range, and on telemetry from missile tests, which take

place at unpredictable times. They are therefore parked in geosynchronous orbits. Once in orbit, a Rhyolite unfolds a dish-shaped receiving antenna approximately 70 feet (21 m) across and begins listening. From its altitude of over 22,000 miles (35,400 km), a Rhyolite can pick up walkie-talkie conversations on Earth—and perhaps even weaker signals.

Other large, geosynchronous SIGINT satellites have been orbited by the U.S., with missions similar to Rhyolite's. Also, as mentioned above, the KH-11 and KH-12 series satellites have carried SIGINT as well as photoreconnaissance equipment. There is little that is transmitted electronically that cannot be intercepted by the United States's SIGINT satellites. The Soviet Union also launched numerous SIGINT satellites, emphasizing continuous coverage of the oceans and of North Atlantic Treaty Organization (NATO) countries by networks of low-orbiting satellites rather than by fewer, more sensitive satellites in geosynchronous orbits. Like other spy-satellite assets inherited by the Russian Federation from the Soviet Union, these SIGINT resources have degraded steadily, with many satellites falling out of service without replacement.

An important class of SIGINT satellites is dedicated to characterizing on-the-ground radar systems, including early-warning, missile-tracking, naval, civil, and other radars. Because radar systems are *designed* to radiate large amounts of electromagnetic energy, their detection is straightforward compared to the gathering of COMINT, and relatively small, cheap satellites suffice. Satellites or aircraft that specialize in characterizing enemy radars are termed "ferrets." Many ferrets have been launched since the first U.S. ferret in May 1962; some experts estimate that SIGINT satellites, including ferrets, are about four times as numerous as photoreconnaissance satellites. At least eight U.S. ferrets are orbiting the Earth at any one time, many in geosynchronous orbits or in highly elliptical orbits. The advantage of an elliptical orbit for ferreting is that when the satellite is near its apogee (i.e., when it is farthest from the Earth), its velocity is very low. By positioning the orbit so that its apogee is above an area of interest, Siberia, for example, the satellite can be made to "hang" for hours above that area, gathering continuous data. At the same time, elliptical orbits do not require as much energy to achieve as geosynchronous orbits, and so are cheaper.

Radar Satellites. Both the U.S. and the Soviet Union have launched satellites that map the Earth and track ships at sea using radar. Radar satellites, unlike visual-light satellites, can image at night and through clouds. Orbital radar imaging was first tested by the U.S. on a 1984 flight of the space shuttle *Challenger*, and was used with great success by the Magellan mission to Venus, launched 1989. Beginning in 2008, an ambitious U.S. program dubbed Discoverer II will orbit a constellation of low-orbit satellites called the Space-Based Radar (SBR) Objective System. The 24 satellites of the SBR Objective System will provide continuous, real-time, high-resolution radar imaging of the entire world, additionally supplying super-high-resolution imaging of a smaller area using side-looking synthetic-aperture radar (SAR). The ordinary radar footprint (area of view) of an SBR Objective System satellite will be a circle about the width of the continental United States; the footprint of its SAR will be about a quarter as large, shaped like a pair of butterfly wings aligned with the direction of travel of the satellite. These "wings" will slide along the ground with the satellite, defining a double track of territory that can be mapped by SAR. The SBR Objective System will provide real-time precision terrain mapping and tracking of vehicles moving on the ground, in the air, or at sea. (Radar cannot penetrate water, so submarines will not be observed.) Unlike older photoreconnaissance systems, which transmitted their information solely to centralized interpretation centers, information from the SBR Objective System will also be downlinked directly to commanders in the field. Testing of SBR Objective System satellite prototypes begin in 2004.

Space-Based Infrared Satellite Systems. An important U.S. satellite system that is now in the process of development is the Space-Based Infrared Satellite System (SBIRS), which is intended to replace the aging DSP early-warning system. SBIRS is intended not only to detect launches, but also to provide detailed tracking information that could be used in antiballistic missile defense. SBIRS will have two components, SBIRS High and SBIRS Low. SBIRS High will consist of satellites in geosynchronous and highly elliptical orbits, much like DSP, but with increased sensitivity. SBIRS Low will consist of a constellation of low-orbit satellites—probably 24, like the SBR Objective System—that will use infrared sensors to track missiles' trajectories for the purpose of guiding defensive systems such as interceptor missiles. Whether the proposed antiballistic missile system of which SBIRS Low would be a part would be effective is technically controversial. The first SBIRS High satellite was scheduled for launch in 2003, and the first SBIRS Low for about 2008.

Other developments. Although the U.S. and the Soviet Union had a monopoly on satellite launches during the 1960s, this began to change in 1970, when both China and Japan orbited their first satellites. Neither was a spy satellite: Japan had vowed to conduct a strictly nonmilitary space program, while the Chinese launch, like the Soviet Union's 1957 Sputnik, was a demonstration. (Its sole function was to broadcast a tape recording of the Chinese Communist anthem, "The East Is Red"). However, China was soon launching military satellites, and by 1999, claimed to possess a network of 17 spy satellites that monitor the U.S. military continuously. Japan launched its first two spy satellites in 2003, breaking its self-imposed ban on military space projects in order to spy on North Korea's

efforts to develop ballistic missiles and nuclear weapons. India launched its first spy satellite, the Technology Experiment Satellite (officially experimental, but viewed by space experts as a surveillance platform) in 2001.

Israel orbited its first spy satellite (Ofek 3, a photo-reconnaissance platform) in April 1995. For about one and a half years in 2000–2002, the demise of Ofek 3's successor, Ofek 4, left Israel without a national spy satellite system. During that period, it compensated by buying high-quality imagery from a civilian U.S. Earth-imaging satellite, Landsat. The quality of such imagery approaches that of the best spy-satellite imagery available to the U.S. or Soviet Union during the 1960s. As images from Landsat, Ikonos (a commercial U.S. satellite launched in 1999), and the French-owned SPOT (Système Probatoire d'Observation de la Terre) satellites are now available, anyone who can afford the per-image cost now has, in effect, significant satellite capability, whether for scientific or military purposes. Surveillance is in the eye of the beholder: an image is an image, whether produced by a "nonmilitary" or "spy" satellite. This was underlined during the U.S. war with Afghanistan in October 2001, when the U.S. government took the unprecedented step of buying exclusive rights to all Ikonos satellite images of Afghanistan in order to prevent them from being purchased by media outlets. It is likely that space imagery will continue to become more widely available as launch capabilities and imaging satellites proliferate, making it less feasible to control its distribution.

Just as nonmilitary orbital imaging systems are increasingly of military significance, military imaging systems are increasingly finding nonmilitary application. The DSP satellites have greatly augmented astronomers' catalogs of infrared stars. The SBIRS may be used to catalogue near-Earth asteroids to predict and possibly fend off a catastrophic collision; and after the loss of the space shuttle *Columbia* in 2003, NASA contracted with the U.S. National Imagery and Mapping Agency to routinely photograph shuttles in flight.

■ FURTHER READING:

BOOKS:

Burrows, William E. *Deep Black: Space Espionage and National Security.* New York: Random House, 1986.

PERIODICALS:

Campbell, Duncan. "U.S. Buys up All Satellite War Images." *The Guardian (London).* October 17, 2001.

Dooling, Dave. "Space Sentries." *IEEE Spectrum* (September, 1997): 50–59.

Duchak, G. D. "Discoverer II: A Space Architecture for Information Dominance." *Aerospace Conference Proceedings* (Vol. 7), IEEE, 1998: 9–17.

Forden, Geoffrey, Pavel Podvig, and Theodore A. Postol. "False Alarm, Nuclear Danger." *IEEE Spectrum* (March, 2000): 31–39.

Slatterly, James E., and Paul R. Cooley. "Space-Based Infrared Satellite System (SBIRS) Requirements Management." *Aerospace Conference Proceedings* IEEE, 1998: 223–32.

SEE ALSO

Ballistic Missiles
Balloon Reconnaissance, History
Electronic Communication Intercepts, Legal Issues
Electro-Optical Intelligence
Geospatial Imagery
GIS
Global Communications, United States Office
IMINT (Imagery intelligence)
Intelligence and International Law
Mapping Technology
Photographic Interpretation Center (NPIC), United States National
Reconnaissance
Remote Sensing
Satellite Technology Exports to the People's Republic of China (PRC)
Satellites, Non-Governmental High Resolution
United States, Counter-terrorism Policy
Weapons of Mass Destruction, Detection

Saudi Arabia, Intelligence and Security

The Middle East is the seat of some of the world's most ancient civilizations and ethnic groups. Ancient Persia (Iran) and Byzantium (Turkey), in different eras, both claimed the land corresponding to present-day Saudi Arabia. These civilizations had complex government structures, which included developed bureaucracies and some of the earliest intelligence communities.

Abd al-Aziz Saud established the nation of Saudi Arabia in 1920 when he captured the city of Riyadh. He and his forces then began a three-decade campaign to unify tribal lands and city-states in the Arabian Peninsula. The quest was aided by the discovery of oil in the region during the 1930s, which produced great wealth for the royal family and Saudi Arabia. Today, the royal family remains in control of Saudi Arabia and the daily operations of its government. Because of its strategic location and its vast oil wealth, Saudi Arabia maintains one of the largest and most sophisticated intelligence communities in the Middle East.

In recent years, the Saudi government and intelligence services have become more concerned with the influx of refugees and immigrants. Increasing global concern over Islamist terrorist networks, and international suspicion of Saudi officials for permitting the funneling of

weapons and money through Saudi Arabia, prompted closer monitoring of Saudi national borders. Saudi intelligence and security forces erected video surveillance cameras, night vision and thermal cameras, and next-generation radar along national borders and the coastline. The electronic surveillance is meant to aid an extensive troop force, and free some military personnel for other operations. The government also offers incentives and high monetary awards for citizens who aid in the identification and arrest of illegal aliens.

Saudi civilian intelligence is directed by the Ministry of the Interior and Ministry of Interior Forces. The Directorate of Intelligence coordinates all civilian and some military intelligence operations. Both foreign and domestic intelligence information is collected and processed by the Directorate, which in turn works closely with Saudi Arabia's many police forces.

The Saudi government maintains several law enforcement agencies with ties to the intelligence community. The Directorate of Investigation investigates suspicious activity, conducts anti-terrorism and anti-crime surveillance, and has operational units to participate in security operations and political espionage. The Committees for the Propagation of Virtue and the Prevention of Vice (religious police) enforce the nation's tough anti-trafficking and drug laws, as well as social laws on modesty of dress and media censorship. The Public Security Police is the main national law enforcement agency, dedicated to preserving public safety and national security.

In addition to civilian forces, the Saudi military has extensive intelligence forces. The main agency for military and foreign intelligence is the G-2 Intelligence Section. The Ministry of Defense coordinates military intelligence and security operations, most of which are secret. Saudi military forces utilize the advanced surveillance and espionage technology in the region, gathering a wide range of electronic, signals, communications, remote, and human intelligence information.

In 1990 Saudi Arabia permitted the Kuwaiti royal family to flee the Iraqi invasion of Kuwait and establish an exile government in Saudi Arabia. In 1991 Saudi Arabia permitted the United States military to use its territory as a staging ground to launch an attack against Iraqi occupying forces in Kuwait in the Persian Gulf War. However, the Saudi government, at least publicly, opposed coalition military action against Iraq in 2003.

■ FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. "CIA World Factbook, Saudi Arabia." <http://www.cia.gov/cia/publications/factbook/geos/sa.html> (March 29, 2003).

SEE ALSO

Persian Gulf War

Scanning Technologies

■ LARRY GILMAN

X rays are electromagnetic waves in the 10^{-8} to 10^{-11} meter (3×10^{16} to 3×10^{19} Hz) range of the spectrum. (Alternatively, x rays can, like all electromagnetic waves, be conceived of as particles termed "photons.") Because x rays have more energy than visible light, they can pass through solid objects that are otherwise opaque. However, they do not, in general, pass through them as if they almost transparent, as air is to visible light; rather, when x rays encounter materials of different densities and compositions, they are absorbed and deflected from their original straight-line paths (scattered) to different degrees. This allows x rays to be used for imaging the interiors of many objects. The two commonest commercial applications of x-ray scanning technology are medical imaging of the interior of the body and security scanning of baggage and cargo.

Projection radiography. Projection radiography (also termed transmission imaging or fluoroscopy), discovered in 1895, is the oldest and simplest form of x-ray scanning. In projection radiography, a beam of x rays is directed at an object behind which a detector or x-ray sensitive surface (i.e., electronic-device array or photographic film) is placed. Volumes of different absorptive properties in the object absorb and scatter the incident x rays to different degrees, causing an x ray shadow to be cast on the detecting surface. This shadow pattern is the x-ray image.

There are two essential limitations on projection radiography: first, it can readily resolve only structures that contain strong x-ray absorption contrasts. In human beings, this means that the soft tissues are difficult, or impossible, to image. Second, all three-dimensional structure in the x-rayed object is collapsed or flattened onto the image plane, destroying information. Nevertheless, because of their speed, simplicity, and economy, projection-type x-ray systems are still commonplace in hospitals and standard in security systems that examine cargo, baggage, and other inanimate objects. Airports rely heavily on projection-type x-ray machines to examine carry-on luggage and checked baggage for explosives and weapons. X raying of passengers, however, has until recently, been out of the question due to the negative health effects of x-ray radiation. X-ray photons are ionizing, that is, can knock electrons loose from atoms, disturbing whatever chemical bonds the atom may happen to be participating in. In a living system, ionization causes toxicity and genetic damage; at low levels it increases cancer risk and at high levels causes radiation sickness or death. At beam intensities high enough for rapid imaging of travelers, x rays would significantly increase long-term cancer risk. Fetuses and

A Transportation Security Administration screener, left, loads luggage into an x-ray scanner at the Bismark, North Dakota, airport. More than 30,000 new Security Administration employees were hired for increased airport security screening since the September 11, 2001, terrorist attacks on the World Trade Center in New York. AP/WIDE WORLD PHOTOS.

infants are especially vulnerable to all ionizing radiation, including x rays.

Computed tomography. Computed tomography (CT, also known as computerized axial tomography, CAT) was first made commercially available in the mid-1970s. CT combines projection radiography with computer processing to recover the three-dimensional information that is lost in a traditional two-dimensional x ray. In a CT scanner, the object to be scanned (e.g., person or baggage item) is placed in a cylindrical or doughnut-shaped device. Inside the cylinder or doughnut is an x-ray source that is mechanically rotated entirely around the object. Also, the cylinder or doughnut is lined with detectors that measure the x rays that pass through the scanned object at all angles. By collating all the information that is gathered during a full revolution of the x-ray source, a computer can form a three-dimensional model of the irradiated volume of the object. This information can then be presented to the user on a video screen in any desired form; most commonly, a thin slice of the object is modeled, with the details of its structure imaged as a black-and-white cross-section. To examine more of the object, the user looks at multiple slices.

CT scanning provides information not only on gross structure but on material density. In medical applications, this enables it to image soft tissues far better than conventional x-ray systems. In some security CT systems, the scanner's computer can automatically color-code densities characteristic of explosives or other special substances.

CT scanning is computation-intensive and requires rotation of the x-ray source around the scanned object, making this technique slower and much more expensive than transmission-type imaging. However, because CT images not only the geometry but the density distribution of complex three-dimensional structures, including (potentially) explosives shaped into thin sheets and other devices structured to avoid detection, most U.S. airports have one or more CT scanners. Since it is not practical to put all bags through the CT scanner, only selected or "suspicious" bags (e.g., those belonging to a passenger who pays cash for a one-way ticket) are passed through the CT scanner. Technological improvements in CT scanning are likely to make routine CT scanning of all luggage, with automated computer scanning for weapons or contraband, a reality at airports in some wealthy countries.

Backscatter imaging. "Backscatter" consists of waves that are reflected back from an obstacle. In backscatter imaging, x rays are beamed at a target object and a sensor co-located with the beam source records reflected (backscattered) waves. Since denser objects tend to create more backscatter, backscatter x-ray systems create a density-contrast image that reveals different information about objects' interiors than does transmission imaging. Because transmission imaging and backscatter imaging can provide complementary information, relocatable military x-ray systems designed to inspect entire cargo containers, trucks, helicopters, and the like (e.g., the U.S. military's Isosearch system) acquire both transmission and backscatter images.

Backscatter imagers for personnel have also been constructed. A typical walk-through backscatter x-ray system can see what is beneath a person's clothing—including the person. Although this is useful for detecting hidden weapons, it also raises obvious questions of privacy and legality where use on the general public, such as in airports, is proposed. There are also, as with all x-ray imaging modalities, health concerns. Although a walk-through of a backscatter imaging system would expose a person to only about 1/7,000 of the dose of a conventional medical x ray, some health physicists argue that frequent flyers and women who are pregnant but do not yet know it might still receive unacceptable cumulative doses from backscatter systems. (High-altitude air travel already increases a traveler's exposure to x rays from space.) Backscatter x-ray systems have been deployed since the late 1990s in a few prisons as alternatives or aids to frisking, and have been found effective.

Stereoscopic x-ray screening. Using specially-constructed sensors it is possible to acquire transmission-type x ray information that can be formed into stereoscopic images (that is, a left-eye, right-eye image pair that the user's brain combines into a three-dimensional impression). Because such an image has apparent depth but cannot be rotated, it is sometimes referred to as "2 1/2 dimensional."

Stereoscopic x-ray technology is only a few years old, but may eventually replace conventional two-dimensional baggage scanners in airports because it provides the operator with additional visual-recognition cues that should increase their chances of correctly identifying weapons. Furthermore, stereoscopic x-ray scanning is quicker and cheaper than CT scanning, as it requires less computation and does not need to rotate the x-ray source around the object being scanned. Its limitations are that it provides neither fully rotatable three-dimensional knowledge of an object nor density data, both of which are provided by CT scanning.

Coherent scattering. The atomic orderliness of a substance affects the way in which x rays are diffracted (i.e., forced to mutually interfere) when passed through it. By recording the scattering patterns characteristic of specific compounds (e.g., drugs, explosives), and comparing these templates to patterns observed when scanning objects, a substance-specific detection system can be devised. This technique is now in the early development stage, and is not ready for deployment.

Other imaging modalities. Several other techniques for imaging object interiors exist, including ultrasound, positron emission tomography (PET), nuclear magnetic resonance (NMR) imaging, nuclear quadrupole resonance (NQR) scanning, and neutron emission analysis. All, like x-ray scanning, have security, medical, or scientific applications; the question of which technique is best for any given application is decided based on physics (i.e., which imaging modalities can do a particular job) and, if more than one technique is usable for a given task, on economics (i.e., which imaging modality yields the minimum acceptable image quality for the least cost). For enhanced efficacy, airport security systems are now being planned that will combine complementary techniques to increase the probability of weapon or contraband detection. Such a system might combine x-ray scanning for suspicious-object detection with neutron emission analysis for chemical identification.

FURTHER READING

PERIODICALS:

Bruning, Horst, and Stephen Wolff. "Automated Explosive Detection Systems Based Upon CT Technology." *Security Technology* 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference on. Oct. 12–14, 1998: 55–58.

Evans, J. P. O., M. Robinson, and S. X. Godber. "Pseudo-Tomographic X-Ray Imaging for Use in Aviation Security." *IEEE AES Systems Magazine* July, 1998.

SEAL Teams

Ranking among the most elite fighting forces in the world, United States Navy SEALs (Sea, Air, Land) operate in teams designed to wage unconventional warfare, particularly in a water environment. The SEAL team concept has its roots in World War II, though actual SEAL teams were not commissioned until 1962. SEAL training, conducted at the Naval Special Warfare Center in Coronado, California, is among the most rigorous programs of military education in the U.S. armed forces. SEAL team operations are noted for their mobility, swiftness, and precision.

In the spring of 1943, the U.S. Navy called for volunteers from its construction battalions (SeaBees) to form

U.S. Navy SEALs join their Filipino counterparts during a 2000 joint counter-terrorism exercise in a remote Philippine village, aimed at helping Philippine forces to destroy the Islamist extremist terror group Abu Sayyaf. AP/WIDE WORLD PHOTOS.

special naval combat demolition units whose mission was to reconnoiter and clear beach obstacles for troops making amphibious landings. These teams, which served with distinction in both the Atlantic and Pacific theatres of war, became known as underwater demolition teams (UDTs) in Korea. There they took part in the landing at Inchon and engaged in a number of missions involving demolition of bridges and tunnels accessible from the water.

In the early 1960s, as the United States increased its involvement in Vietnam, each military service formed a special warfare unit. In 1962 the Navy SEALs gained formal existence with the commissioning of two SEAL teams, One and Two, which served in the Pacific and Atlantic respectively. In 1983 all UDTs and other naval special-warfare teams were redesignated either as SEAL teams or SEAL delivery vehicle teams. On April 16, 1987, the Naval Special Warfare Command at the Naval Amphibious Base was commissioned to prepare naval special warfare forces through training, doctrine, tactics, and the development of special operations strategy.

Among the most significant activities at Coronado is Basic Underwater Demolition/SEAL (BUD/S) training, a rigorous program that culminates in the notorious "hell week." During the latter, prospective SEALs are only allowed about four hours' sleep and must undergo numerous drills that require, among other challenges, heavy lifting, crawling in wet sand with live ammunition fire overhead, and immersion in ice-cold water.

FURTHER READING:

BOOKS:

Boehm, Roy, and Charles W. Sasser. *First SEAL.* New York: Pocket Books, 1997.

Bosiljevac, T. J. *SEALs: UDT/SEAL Operations in Vietnam.* New York: Ivy Books, 1991.

Chalker, Dennis C., and Kevin Dockery. *One Perfect Op: An Insider's Account of the Navy SEAL Special Warfare Teams.* New York: Morrow, 2002.

ELECTRONIC:

Naval Special Warfare. <http://www.sealchallenge.navy.mil> (April 1, 2003).

Navy SEALs.com. <http://www.navyseals.com> (April 1, 2003).

SEE ALSO

Delta Force
Special Operations Command, United States

Secret Codes.

SEE *Enigma.*

U.S. Navy SEALs found intelligence information, including mine recognition posters, located in an al-Qaeda classroom during a Sensitive Site Exploitation mission in the Zhawar Kili area in eastern Afghanistan in January 2000. AP/WIDE WORLD PHOTOS.

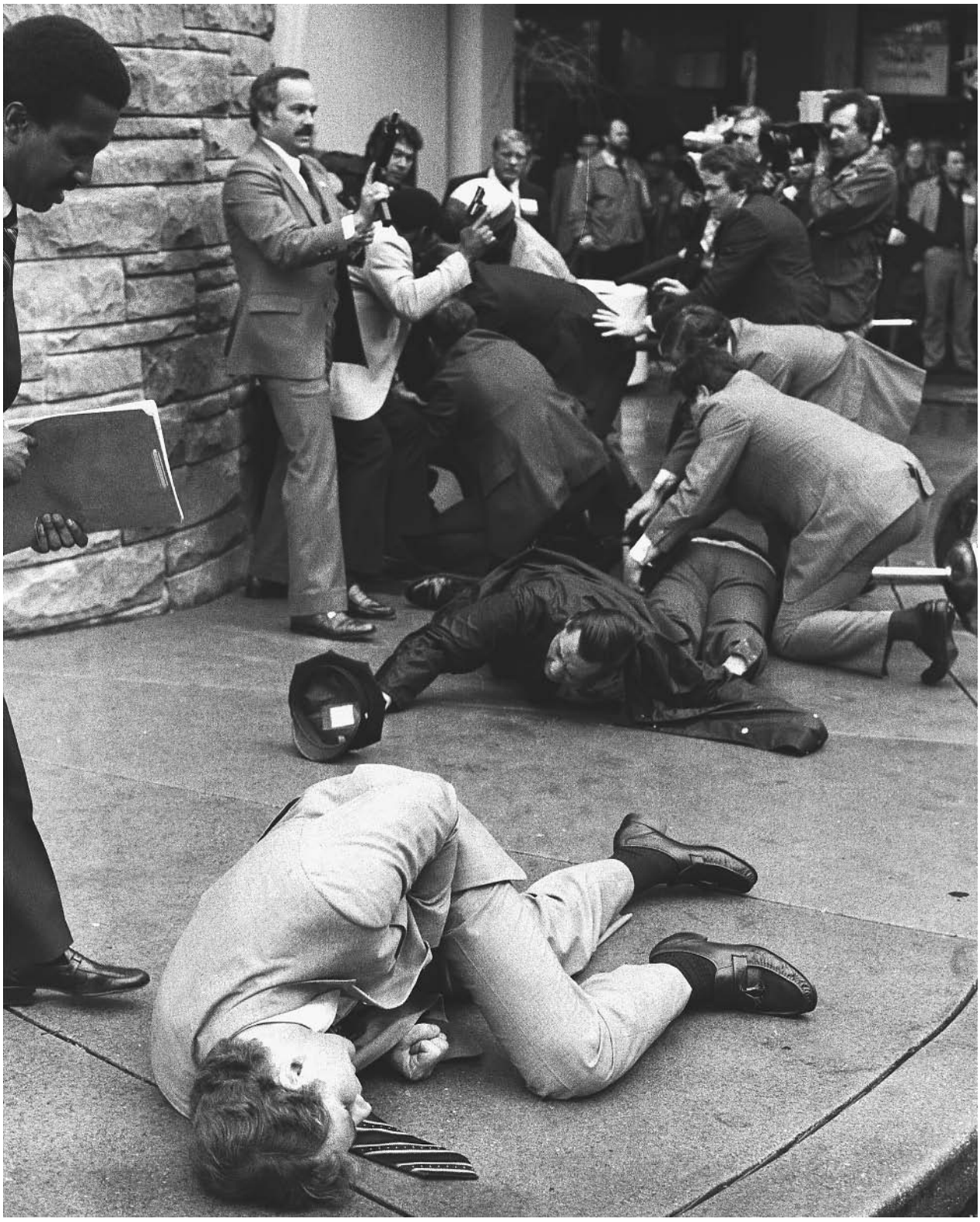
Secret Service, United States

The United States Secret Service (USSS) has two missions that, while sharply distinguished from one another, are united by the principle of protection. On the one hand, in its more visible role, the service provides protection of the president, vice president, and other dignitaries and their families. On the other hand, USSS's larger mission protects securities, including federal currency and other documents. Established in 1865 as an office under the Department of the Treasury, USSS was transferred in 2003 to the newly created Department of Homeland Security (DHS).

Early history. At the time Secret Service was founded, approximately one-third of all currency in circulation was counterfeit. Only in 1877 did Congress pass its first law against the production of counterfeit currency, and even then, the law only encompassed counterfeit coins. By then, the mission of USSS had broadened, with an order in 1867 charging it with "detecting persons perpetrating frauds against the government"—a mission that soon put the service on the trail of a range of lawbreakers ranging from bootleggers to members of the Ku Klux Klan.

The personal protection mission of USSS had its beginnings in 1894, when it first provided protection to President Grover Cleveland on an informal and part-time basis. Following the assassination of President William McKinley in 1901, Congress officially requested USSS protection for presidents, and in 1902 the Secret Service assumed full-time protective duties for the Chief Executive. At that time, the White House detail numbered just two agents.

The first half of the twentieth century. In 1908 President Theodore Roosevelt transferred eight USSS agents to the Department of Justice, where they formed a small contingent that would ultimately become the Federal Bureau of Investigation (FBI). Congress in 1913 authorized USSS to provide permanent protection to U.S. presidents, and in



Secret Service agent Timothy J. McCarthy, foreground, lies wounded outside a Washington hotel after throwing himself in the line of fire of gunshots directed at President Ronald Reagan on March 30, 1981. Washington policeman Timothy Delahanty, center, and Press Secretary James Brady, back, were also wounded along with the president. All those pictured survived their wounds, and McCarthy later returned to duty. AP/WIDE WORLD PHOTOS.

1917 it assigned them to protect presidents' immediate families as well. Also in that year, it became a federal crime to make threats against the president. At the request of President Warren G. Harding, a White House police force was created in 1922, and in 1930 Congress placed this force under USSS direction.

On November 1, 1950, Puerto Rican nationalists attempting to assassinate President Harry S Truman shot and killed White House police officer Leslie Coffelt. This led Congress to pass legislation formalizing USSS permanent protection for presidents and their immediate families, as well for the president-elect and the vice president. In 1962 Congress again expanded these provisions to include the vice president-elect.

The modern Secret Service. After the assassination of President John F. Kennedy on November 22, 1963, awareness of the threat to presidents' lives increased dramatically. The mission of USSS also expanded with regard to the persons under its protection. Congress in late 1963 authorized protection for Mrs. Kennedy and her children for two years, and legislation in 1965 provided protection for a president's spouse, as well as minor children until the age of 16. In June 1968, while on the presidential campaign trail, Kennedy's brother, Senator Robert F. Kennedy, was assassinated. This led to new laws providing Secret Service protection for major presidential and vice presidential candidates and nominees.

The White House Police Force became the Executive Protective Service in 1970, and to its duties was added responsibility for protecting diplomatic missions in Washington, D.C. In the next year, visiting heads of state or government, as well as other official guests, were granted USSS protection. By 1975, the Executive Protective Service was detailed to guard foreign diplomatic missions throughout the United States and its territories. On November 15, 1977, the Executive Protective Service became the Secret Service Uniformed Division, and in October 1986 it absorbed the Treasury Police Force.

Since the Kennedy assassination, only three persons under Secret Service protection have been the target of direct assassination attempts: Alabama governor and third-party presidential candidate George Wallace in 1972, President Gerald Ford in 1975 (twice), and President Ronald Reagan in 1981. All three survived, a circumstance that—particularly in the last instance, when several agents were wounded—owed much to the work of Secret Service.

From the 1980s onward. At the same time, USSS continued work in its other field, protecting securities. In 1984 Congress made credit- and debit-card fraud a federal violation, and authorized Secret Service to investigate those crimes, as well as fraud involving identification documents. USSS in 1990 received concurrent jurisdiction with Department of Justice law enforcement personnel to conduct civil and criminal investigations relating to federally insured financial institutions. In 1994 new legislation provided for the prosecution of persons counterfeiting U.S. currency abroad, assessing them with the same penalties as if they had committed the crime on American soil.

Also in 1994, Congress reduced the lifetime-protection provisions for presidents. All chief executives elected after January 1, 1997, would receive protection only for the first 10 years after leaving office. Under the provisions of the Homeland Security Act of 2002, Secret Service moved to the new DHS.

Though its headquarters are in Washington, D.C., just three blocks from the White House, Secret Service operates more than 120 field offices in all 50 U.S. states. It also has more than a dozen offices in foreign countries. It employs 2,100 special agents, another 1,200 uniformed agents, and some 1,700 support personnel.

Uniformed and special agents. Requirements for special agents are somewhat higher than for uniformed officers—for example, a bachelor's degree is a condition of eligibility for the former and not the latter—but standards for both are high, and applicants must pass an extensive series of tests and background checks. Those selected by Secret Service undergo a nine-week training course at the Federal Law Enforcement Training Center in Glynco, Georgia, followed by specialized training. Special-agent candidates take an additional 11-week course at the Secret Service Training Academy in Beltsville, Maryland. Uniformed officers receive varying types of training.

Agents serving in the Uniformed Division provide protection at the White House and a number of other key sites in Washington. They often work with support teams that include countersniper, emergency response, and canine units. Special agents usually spend their first six to eight years in a field office, then are assigned to provide personal protection for three to five years. After this assignment, they may choose a number of paths, continuing in a protective detail, serving in the field, or working in some other capacity.

■ FURTHER READING:

BOOKS:

Department of the Treasury. *Excerpts from the History of the United States Secret Service, 1865–1875.* Washington, D.C.: Department of the Treasury, 1978.

McCarthy, Dennis V. N. with Philip W. Smith. *Protecting the President: The Inside Story of a Secret Service Agent.* New York: William Morrow, 1985.

Melanson, Philip H. *The Politics of Protection: The U.S. Secret Service in the Terrorist Age.* New York: Praeger, 1984.

Motto, Carmine J. *In Crime's Way: A Generation of U.S. Secret Service Adventures.* Boca Raton, FL: CRC Press, 2000.

ELECTRONIC:

United States Secret Service. <http://www.ustreas.gov/usss/> (February 5, 2003).

SEE ALSO

Counterfeit Currency, Technology and the Manufacture Engraving and Printing, United States Bureau

Secret Writing

Secret writing is any means of written communication whereby a spy conceals the actual written text, whether it is enciphered/encoded or not. Codes and ciphers are sometimes mistakenly placed under the heading of "secret writing," but this is accurate only if that expression is taken in its most general sense, as writings that are concealed in any way. Whereas codes and ciphers conceal the meaning of a message, secret writing conceals the actual message. Techniques of secret writing include the use of invisible ink and carbon copies. Widely applied from ancient times until the early twentieth century, secret writing has been almost entirely eclipsed by more modern methods of concealing messages, such as microdots.

An early example of secret writing. In his venerable *History,* Herodotus described a method of secret writing employed in the Persian Wars. As the Persian emperor Xerxes was preparing to march on the Greek city-states in 480 B.C., a Spartan expatriate name Demaratus learned of the plans and contrived to warn his compatriots. The problem was how to do so in such a way that the Persians themselves would not intercept the message, a challenge for which Demaratus contrived a clever solution.

As Herodotus recorded, Demaratus scraped the wax from a pair of wooden tablets, wrote his message on the wood beneath, then poured hot wax onto the tablets again. Of course the Spartans lacked the advantage of knowing that they were receiving a secret message, but according to Herodotus—who qualified his claim with the caveat "as I understand [it]"—Gorgo, the daughter of a citizen named Cleomenes, received a divine revelation. Thanks to the intervention of the gods, the Spartans realized that they had simply to scrape off the wax and read the message written on the wood beneath it. The Greeks thus began to prepare for the coming invasion, and routed Xerxes's navies at Salamis.

Invisible ink. One form of secret writing known to many children from school projects is invisible ink. This technique uses an acidic citrus juice, of which lemon juice is most often the preferred choice because it dries without leaving any evidence it has been applied. The juice takes the place of ink, and is applied using a fine stylus (a tool for which an ordinary toothpick will suffice). After the juice dries, the acid remains on the paper, which it weakens, and therefore the message is readily exposed when heat is applied to the paper.

Other liquids for invisible ink include milk, which is mildly acidic, as well as white wine, vinegar, or apple juice. In the past, prisoners of war have used their own sweat, saliva, or even urine, all of which contain acidic secretions that adhere to the paper, weakening it, even after the water in those bodily fluids has evaporated. A slight variation on this technique is the use of a baking soda and water mixture as the invisible ink, and, after drying, applying grape juice concentrate with a paint brush. The acid in the grape juice reacts with the baking soda (a base or alkali in chemical terms), exposing the message.

Carbon copies. During the late nineteenth and early twentieth centuries, carbon copies provided a means of secret writing. This method, which was even used by the Central Intelligence Agency (CIA) in its early days, involved a means not unlike the one still used today when signing a credit-card receipt. The back of the receipt is impregnated with graphite, a carbon allotrope (a version of a chemical element distinguished by molecular structure) also used in pencil lead. Therefore, when one signs the front of the receipt, the pressure transfers the graphite to the second page, leaving an impression as though one had written on it in pencil.

The CIA version of this technique involved paper containing a special chemical that would be invisible when transferred to the second sheet. This made it possible to inscribe secret writing on the back of an envelope, which could be mailed to the agent through ordinary channels. Using water or heat, the message could then be developed and read.

Secret writing today. The use of secret writing has declined since the middle of the twentieth century for several reasons, most important of which is the sheer volume of data that intelligence services must transmit and process. This has prompted the use of more efficient means for concealing information without having to write it out by hand. One such means was the microdot, or miniaturized photographic image. First used in the mid-1800s, microdots remained popular among intelligence services through the 1960s, their use aided by the development of microdot cameras.

Much more sophisticated is the technique of steganography, the concealment of information within other, apparently innocuous, data in a computer file. Yet, old-fashioned secret writing remained enough of a factor in intelligence that in 1990, the Senate Select Intelligence Committee noted its use by persons conducting espionage against the federal government. In 2002 Russian

An FBI agent is shown using ultraviolet light to read secret writing on a paper from a suspected spy case. ©BETTMANN/CORBIS.

authorities claimed that a Russian Defense Ministry employee had passed information to CIA using invisible ink.

FURTHER READING:

BOOKS:

Gardner, Martin. *Codes, Ciphers, and Secret Writing.* New York: Pocket Books, 1974.

Zim, Herbert Spencer. *Codes and Secret Writing.* New York: W. Morrow, 1948.

PERIODICALS:

Ingram, Judith. "Russia Accuses U.S. of Espionage." *Chicago Sun-Times.* (April 11, 2002): 27.

Lardner, George, Jr. "Panel Proposes Tougher Laws against Espionage." *Washington Post.* (May 24, 1990): A16.

SEE ALSO

Cryptology, History
Dead Drop Spike
Dead-Letter Box
Encryption of Data

Security Clearance Investigations

JUDSON KNIGHT

A security clearance is a limited license or initial general permission to access classified information—that is, any data or material belonging to the federal government that relates to sensitive topics such as military plans or vulnerabilities of security systems. Authorization for a security clearance is far from automatic, but rather requires extensive background checks and investigations. A number of laws, including Executive Order 12968, govern

background investigations and security clearances, but numerous aspects of the topic remain controversial. This is equally so for the private sector, in which background investigations as a precondition for employment are an increasingly familiar fixture of the workplace.

There are three levels of security clearance, corresponding to three levels of classified material: *Confidential,* a term referring to information whose disclosure to unauthorized personnel could reasonably be expected to cause damage to national security; *Secret,* or information whose disclosure to unauthorized personnel could result in serious damage to national security; and *Top Secret,* a term referring to information whose disclosure to unauthorized personnel could reasonably be expected to result in exceptionally grave consequences.

Background

In addition to the most basic and widely known levels of security clearance, there are numerous other categories, including "need to know" and "compartment." An individual or agency with a "need to know" has a demonstrable and recognized purpose for accessing specific information. "Compartment," in the context of security clearances, refers to a group of individuals with a need to know regarding a specific topic.

Each "compartment" has its own code words and access keys for computerized information. For example, the Central Intelligence Agency (CIA) has used specific colors on cover sheets to indicate particular compartments. Such agencies may designate information according both to the level of security clearance and the compartment. Thus, for one compartment of CIA in the 1970s, devoted to aspects of intelligence concerning the Soviet Union, a message might be designated TOP SECRET REDWOOD.

Implementation of the "compartment" concept as such—and, indeed, the concept of the security clearance—goes back to the days just before America's entry into World War II. At that time, General George Marshall established a list of persons authorized to receive intelligence obtained through the decoding of Japanese diplomatic transmissions. According to Marshal's "Top List," access to this compartment, designated MAGIC, would be limited to the president; the secretaries of State, War, and the Navy; and the directors of army and naval intelligence. As Jeffrey T. Richelson noted in *The United States Intelligence Community,* "Among those not on the list was the Commander of United States Naval Forces at Pearl Harbor, Admiral Husband Kimmel."

During the war, United States and British intelligence developed a number of compartments, and after signing the Brusa Communications Intelligence Agreement in May 1943, the Allies designated high-level shared information as ULTRA, a term that emerged from British intelligence. Usually ULTRA intelligence would carry a second word designating the compartment: for example, ULTRA RABID referred to traffic analysis intelligence based on intercepted Japanese communications.

In the quarter-century that passed between the beginning of World War II and the height of the Vietnam War, the degree to which the concepts of classified information, compartments, and security clearances matured was nothing short of astounding. Richelson noted this extraordinary development in connection with an interchange during a 1964 Senate Foreign Relations Committee hearing. At the time, the Gulf of Tonkin resolution—which would ultimately give President Lyndon B. Johnson authority to greatly expand the United States presence in Southeast Asia—was under discussion. When committee chairman William Fulbright asked for the source of information on a planned attack by North Vietnamese gun boats against the U.S.S. *Turner Joy* on the night of August 4, Defense Secretary Robert McNamara replied that "We have some problems because the [committee] staff has not been cleared for certain intelligence."

Senator Frank Lausche expressed bewilderment because, as far as he knew, the committee staff had the highest level of clearance, but Fulbright noted that "he [McNamara] is talking of a special classification of intelligence communications." When Senator Albert Gore, Sr., asked McNamara to clarify, saying, "I had not heard of this particular super classification," McNamara replied, "Clearance is above top secret for the particular information on the situation."

Sensitive compartmented information. "Above top secret" might sound like a contradiction in terms, or at least similar to a fantastic invention of a conspiracy buff, but what McNamara referred to was a compartment. As Senate records show, McNamara went on to identify the category of clearance as Special Intelligence, or SI. The latter is in turn part of a category designated Sensitive Compartmented Information (SCI), which the National Foreign Intelligence Board (NFIB) defined in a 1984 report as "data about sophisticated technical systems for collecting intelligence[,] and information collected by those systems." The systems referred to here would include any and all submarines and ships, ground stations, aircraft, and satellites tasked to the gathering on sensitive information.

Within SCI are several compartments, such as TK or TALENT-KEYHOLE, which concerns data gathered from imaging satellites. SCI also has its own levels of security clearance, ranging from MORAY to SPOKE to UMBRA. To these may be added the more traditional designations mentioned earlier, but even a Confidential document at this high level carries much greater restrictions than an ordinary Top Secret document.

Executive Order 12968. One of the most important documents governing access to classified information and the granting of security clearances is Executive Order 12968,

signed by President William J. Clinton on August 4, 1995. Titled "Access to Classified Information," the order "establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information." It provides rules governing access, among which is the requirement that those being considered for such access submit themselves to investigation of financial records. The order calls upon employers to submit the names of employees who might be considered risks for revealing classified information, and to educate employees with regard to their responsibilities to maintain classified information.

At the beginning of Part 2, "Access Eligibility Policy and Procedure," the order provides for strict limitations on the number of employees in a given office who may be eligible for access to classified information, and notes that such eligibility "shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas where the employee has no need for access and access to classified information may reasonably be prevented." Part 3 establishes the standards of eligibility, and Part 4 consists of a single paragraph allowing federal agencies to conduct background investigations on behalf of foreign governments if needed.

Part 5 enumerates the employee's right to appeal in cases where access is denied. If the denial has occurred because the employee has no justifiable need to know, there is no appeal, but if he or she has been deemed wanting according to the standards established in Section 3.1, then the employee has a right to request an explanation, as well as copies of all documents upon which the denial is based, assuming that access to them is permitted under the Freedom of Information Act.

Criticisms of 12968. Despite these provisions, according to the journal *Government Executive,* Executive Order 12968 did not reach as far as some advocated. Federal labor unions and legal experts complain that private sector workers still have more substantial appeal rights "that were unaffected by the executive order." Writing in the same publication, Richard Lardner described the order as the culmination of efforts to prevent another case like that of Aldrich Ames, the CIA employee arrested in 1994 for passing information to the Soviet Union and later Russia. For his efforts, Ames received a total of $2 million from Moscow. If the federal government had possessed greater knowledge concerning Ames's finances, supporters of the new financial disclosure measures maintained, he might have been stopped sooner.

To this end, the order had called for the United States Security Policy Board to develop a financial disclosure form whereby employees could provide information regarding their personal finances. Though the board was given 180 days to develop such a form, Lardner noted, a year and a half had passed without any such document emerging. Furthermore, he argued that there were "plenty of questions as to whether a form makes any sense at all," since "Agents willing to betray their country are no more inclined to fill out a financial disclosure form honestly than they are to turn themselves in."

Background Investigations

Some 3 million federal employees, as well as about 1.5 million employees of private contracting or consulting firms such as General Dynamics or Boeing, hold security clearances of one kind or another. They receive these only after an extensive series of background checks, which may be as intrusive are they are detailed.

Still, there are gaps in the system. Political parties have often resorted to charges that opponents in government office did not legitimately hold appropriate clearances. These charges reached historical peaks during the 1950s "Red scare" and again during the Clinton administration.

Procedures for government employees and contractors. Military personnel and federal employees requesting security clearances are required to fill out Standard Form (SF) 86, "Questionnaire for National Security Positions." The form, which is rather like an extremely lengthy and detailed version of a job application, then goes to the appropriate investigating authority—for example, the Defense Security Service (DSS) for military personnel. If the clearance requested is Confidential or Secret, there will follow computerized checks with federal and state agencies for information on employment, residences, education, and criminal history. A check of credit history is also conducted.

For Top Secret clearance, in addition to these checks of computerized data, the investigating authority also conducts interviews of personal references given on SF 86, including friends, present and former coworkers and employees, present and former neighbors, and others. Investigators use these references to generate others—i.e., acquaintances mutual to the subject and the reference that the subject may not have listed on the form.

Interviews involve questions about past and present activities, family background, finances, and so on, with an eye toward determining whether the individual has a questionable record involving drugs, alcohol, unexplained foreign travel, criminality, mental imbalance, financial malfeasance, or compromising sexual behavior. Additionally, investigators will check the records of employers, courts, and rental offices, and conduct a one-on-one interview with the subject.

Non-governmental background investigations. In the civilian world, background investigations are typically less stringent for a number of reasons. Companies lack both the resources and the power that the federal government has at its disposal, and in any case, it is hard to imagine a situation in which a security breach involving a producer

of game software or soft drinks could impinge on the future of civilization. Nevertheless, non-governmental background investigations can still be quite extensive. Among the devices used by companies to screen employees are drug tests, polygraph tests, medical and physical exams, routine reference checks, and thorough investigations of the individual's criminal history, driving record, financial and credit information, history of civil litigation, and other details. In some cases, investigators may even gather information on the applicant's lifestyle and personal reputation.

Background investigations in the private sector are increasingly big business. Thousands of companies offer their services to investigate virtually every aspect of the job candidate's background, including such sensitive issues as family history. The more thorough private investigators may conduct door-to-door interviews with neighbors, and some even go through the job candidate's trash—which is legal as long as it is on the curb for pickup—to find correspondence, receipts, or other revealing documents or materials.

Naturally, job candidates—especially those disqualified by the results of background checks—have challenged the legality of such activities. Such concerns played a part in the passage of the Fair Credit Reporting Act (FCRA) by Congress in September 1997. The FCRA requires potential employers to obtain written authorization from a job candidate or employee before accessing records from a consumer-reporting agency, and to notify the employee or applicant is any adverse action is taken pursuant to a negative report. According to a study published in *Public Personnel Management,* background and reference checks are potentially so risky, in a legal sense, to employers that many consider alternatives such as personality tests.

FURTHER READING:

BOOKS:

The Guide to Background Investigations: A Comprehensive Source Directory for Employee Screening and Background Investigations. Tulsa, OK: T.I.S.I., 1998.

Newman, Elizabeth L. *Security Clearance Law and Procedure.* Arlington, VA: Dewey Publications, 1998.

Richelson, Jeffrey T. *The United States Intelligence Community,* third edition. Boulder, CO: Westview Press, 1995.

PERIODICALS:

"Access Denied." *Government Executive* 29, no. 2 (February 1997): 19.

Bland, Timothy S. "Background Checks: Making a Federal Case." *Journal of Property Management* 64, no. 5 (September/October 2000): 26–31.

Lardner, Richard. "The Need to Know." *Government Executive* 29, no. 2 (February 1997): 16–21.

Terpstra, David E., et al. "The Nature of Litigation Surrounding Five Screening Devices." *Public Personnel Management* 29, no. 1 (spring 2000): 43–54.

SEE ALSO

Ames (Aldrich H.) Espionage Case
Classified Information
Clinton Administration (1993–2001), United States National Security Policy
Executive Orders and Presidential Directives
Privacy: Legal and Ethical Issues

Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator

The U.S. National Coordinator for Security, Infrastructure Protection, and Counterterrorism is a broadly based office created by Presidential Decision Directive (PDD) 62. Signed by President William J. Clinton on May 22, 1998, PDD 62 authorized the national coordinator to oversee policies and programs in areas ranging from counterterrorism to protection of critical infrastructure (such as computers) to consequence management for weapons of mass destruction.

Known as the Combating Terrorism directive, PDD 62 drew attention to the growing threat of unconventional attacks against the United States. On the same day he issued PDD 62, Clinton signed PDD 63, which created the Critical Infrastructure Assurance Office (CIAO). Though the functions of CIAO and the national coordinator were similar, they reported along quite different chains of command. Whereas CIAO, now part of the Department of Homeland Security (DHS), was then part of the Department of Commerce, the national coordinator reported to the National Security Council (NSC).

Given the fact that the NSC is the president's advisory board on national security affairs, this fact signaled the importance of the new national coordinator. So, too, did Clinton's appointment of Richard A. Clarke, who had served in the State Department of presidents Ronald Reagan and George Bush, and would later receive an appointment as special advisor for cyberspace security under George W. Bush.

Bush kept Clarke, famous for warning of a possible "electronic Pearl Harbor" (that is, a terrorist cyberattack) during the Clinton years, on the NSC. Meanwhile, the appointment of four-star general Wayne A. Downing to take Clarke's place as national coordinator further reinforced the importance of the office. Despite their involvement with the NSC, both the national coordinator and the special advisor for cyberspace security came under the newly created DHS.

■ FURTHER READING:

PERIODICALS:

Verton, Dan. "National IT Protection Plan Update Delayed." *Computerworld.* 35, no. 41 (October 8, 2001): 12.

ELECTRONIC:

Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counterterrorism. Federation of American Scientists. <http://www.fas.org/irp/news/1998/05/980522-wh3.htm> (March 26, 2003).

Summary of PDD 62 and PDD 63. Critical Infrastructure Assurance Office. <http://www.ciao.gov/resource/pdd6263summary.html> (March 26, 2003).

SEE ALSO

Critical Infrastructure
Critical Infrastructure Assurance Office (CIAO), United States
Cyber Security
Homeland Security, United States Department
NSC (National Security Council)
United States, Counter-terrorism Policy

Security Policy Board, United States

An advisory committee created by President William J. Clinton in 1994, the Security Policy Board (SPB) reported to the president through the National Security Advisor on matters of security policy. Its short existence was a troubled one, with critics charging that the board's organizational system was too complex and cumbersome. In 2001 the new administration of President George W. Bush abolished the SPB.

On September 16, 1994, Clinton signed Presidential Decision Directive 29 ("Security Policy Coordination"), in which he redesignated the Joint Security Executive Committee, established by the deputy Secretary of Defense and the Director of Central Intelligence (DCI), as the SPB. The latter included the DCI and deputy Secretary of Defense, the vice chairman of the Joint Chiefs of Staff, the deputy Attorney General, and deputy secretaries or undersecretaries of State, Energy, and Commerce. Its job was to consider policy directives and to review and propose legislative initiatives and executive orders relating to U.S. security policy. Additionally, it would coordinate interagency agreements and resolve conflicts over these.

In addition to the board itself, there was a Security Policy Advisory Board, a Security Policy Forum, an Overseas Policy Board (formerly the Department of State Overseas Security Policy Group), and their various interagency working groups. The result was an extremely cumbersome system in which, charged Richard Lardner of *Government Executive,* little was getting done. As of March 1998, the board itself had met only once, in March 1996, and most of its activities took place through various subcommittees and working groups.

The SPB in early 1998 reviewed ties between Commerce Department official John Huang and the Chinese government, and in 1999 severely criticized cost-cutting measures by the Defense Security Service that had resulted in the granting of security clearances to unqualified personnel. On February 13, 2001, Bush dissolved the SPB and other aspects of Clinton's national security structure with National Security Presidential Directive 1, "Organization of the National Security System."

■ FURTHER READING:

PERIODICALS:

Lardner, Richard. "Keeping Secrets." *Government Executive* 30, no. 3 (March 1998): 27–29.

Pound, Edward T. "Security Panel Has Opposed Agency's Cost-Cutting Moves." *USA Today.* (August 20, 1999): 8A.

White, Ben. "Commerce Secretary Unveils New Security Policy." *Washington Post.* (February 11, 1998): A19.

ELECTRONIC:

Security Policy Board Documents. Federation of American Scientists. <http://www.fas.org/sgp/spb/> (April 2, 2003).

SEE ALSO

Bush Administration (2001–), United States National Security Policy
Chinese Espionage against the United States
Clinton Administration (1993–2001), United States National Security Policy
Defense Security Service, United States

Security Screeners.

SEE *Aviation Security Screeners, United States.*

Seismograph

■ LAURIE DUNCAN

A seismograph is an instrument that measures and records elastic ground vibrations called seismic waves that are generated by earthquakes and man-made explosions. By recording the arrival of seismic waves at remote seismograph stations, seismologists deduce information about the initial earthquake fault rupture or explosion, and about the physical properties of earth materials between the seismic source and the seismograph. Much of our present

knowledge of Earth's large-scale interior structure came from analysis of seismograph records. Academic, petroleum, and mining geologists use other seismic techniques to study the structure of Earth's outer sedimentary layers, to prospect for petroleum, and to assess mineral ore bodies. Academic seismograph networks designed to detect earthquakes or planned survey explosions also perform double-duty as monitoring systems that detect military explosions that may indicate violations of international weapons bans.

A modern seismograph includes five basic parts: a clock, a sensor called a seismometer that measures intensity of shaking at the instrument's location, a recorder that traces a chart, or seismogram, of the seismic arrivals, an electronic amplifier, and a data recorder that stores the information for later analysis. The clock records precise arrival times of specific seismic waves. The seismometer mechanically measures ground movement by comparing the motion of a support structure that moves with the land surface to a stationary or inertial mass. To measure vertical motion, the inertial mass hangs from the support by a spring; to measure horizontal motion it is suspended on a hinge. The recording device registers seismic vibrations with a pen attached to the inertial mass, and a roll of paper that moves along with the Earth's vibrations. As the paper cylinder oscillates and unwinds at a constant rate, the stationary pen traces a seismogram that shows the amplitude and frequency of shock waves that arrive over time. Today's seismographs often contain electronic sensors and recorders that perform these tasks, but the principles of their operation remain the same.

Scientists have used tools to detect ground motion since the ancient Han Dynasty when Chang Heng, a Chinese astronomer and mathematician, invented the first seismometer in about 132 A.D. Heng's "earthquake weathercock" seismoscope consisted of a pendulum that swung inside a jar surrounded by eight balanced dragon heads, each holding a bronze ball in its moveable jaws. During an earthquake, the pendulum would swing away from the approaching seismic waves, hit one of the dragons, and knock the ball out of its jaws, indicating the direction of the shock waves.

Seismographs have undergone considerable refinement since Heng's time. European scientists of the 1700s and early 1800s developed a series of mercury-filled seismoscopes and pendulum seismometers that attempted to measure the amplitude and frequency of seismic waves, as well as their propagation directions. British seismologist, John Milne, and his colleagues developed the first modern seismographs to observe Japanese earthquakes in the late 1800s. Their seismographs, however, recorded only a limited range of wave sizes and seismic events, the instruments were fairly inaccurate, and they required difficult mechanical calibration. German seismologist, Emil Weichert, invented an inverted, mechanically damped pendulum seismometer that considerably improved the sensitivity and accuracy of Milne's seismometer in 1899. In 1906 Boris Golitsyn, a Soviet physicist and seismologist, devised an electromagnetic seismograph that operated without mechanical levers, an enhancement of Weichert's instrument. The first modern seismographs in the United States were installed at the University of California at Berkeley and the Lick Observatory at Mount Hamilton, California in 1877. They recorded the 1906 earthquake that devastated San Francisco.

Development of precise seismographs led immediately to discoveries of Earth's interior structure and delineation of its major physical layers: solid inner core, liquid outer core, solid lower mantle, plastic upper mantle, and rigid lithosphere. British seismologist, Richard Oldham (1858 – 1936) observed that seismic events produce three of different types of waves that travel away from an earthquake focus at different speeds, and named them surface waves, P (Primary or Pressure) waves, and S (Secondary or Shear) waves. Oldham and Weichert confirmed the existence of Earth's core in 1906 by comparing the paths of P waves and S waves through the planet's interior. Yugoslavian seismologist and meteorologist, Andrija Mohorovicic (1857–1936) used seismograph records to define the Mohorovicic seismic discontinuity, or Moho, at the boundary of the iron-rich mantle and the silica-rich crust in 1909. The Danish seismologist, Inge Lehmann, discovered of the boundary between Earth's liquid outer and solid inner core in 1914.

Today, seismologists continue to use seismograph records to make discoveries about Earth's interior structure, to prospect for petroleum and minerals, and to monitor large military explosions. The Incorporated Research Institutions for Seismology (IRIS) consortium, for example, operates the Global Seismograph Network (GSN) of about 120 permanent seismographs that continuously record seismic events around the planet and transmit their data to a publicly available data base. The GSN, like its precursor, the World-Wide Seismograph Network (WWSN), detects all but the smallest earthquakes worldwide, as well as seismic waves emitted by nuclear explosions and detonations of large conventional weapons. The academic members of IRIS provide data and analyses in support of the international Comprehensive Test Ban Treaty (CTBT) that seeks to monitor international weapons tests, and identify treaty violations.

■ FURTHER READING:

BOOKS:

Fowler, C. M. R. *The Solid Earth.* Cambridge: University Press, 1990.

Press, Frank and Raymond Siever. *Understanding Earth* New York: W.H. Freeman and Company, 2000.

ELECTRONIC:

Incorporated Research Institutions for Seismology. "Welcome to the IRIS Homepage." December 3, 2001. <http://www.iris.edu>(December 28, 2002).

United States Geological Survey Earthquake Hazards Program. "Seismology." National Earthquake Information Center and World Data Center for Seismology, Denver. April 5, 2001. <http://neic.usgs.gov/neis/seismology/>(December 28, 2002).

SEE ALSO

Seismology for Monitoring Explosions

Seismology for Monitoring Explosions

WILLIAM C. HANEBERG

Seismology has been an important tool for the remote detection of large explosions, especially underground nuclear tests, for many years and is expected to play an important role in Comprehensive Test Ban Treaty verification. The treaty was signed by President Clinton and other world leaders in 1996, and was subsequently ratified by the United States Congress in 1999.

The Limited Test Ban Treaty of 1963 curtailed nuclear testing in the atmosphere, outer space, and under water, leaving underground testing as the only option. The Threshold Test Ban Treaty, signed in 1974, further banned nuclear explosions larger than 150 kilotons. For that reason, Threshold Test Ban Treaty verification concentrated on estimation of explosion size. Explosions large enough to exceed the 150-kiloton limit create earthquakes that are easily detected by seismometers thousands of kilometers away.

Because the Comprehensive Test Ban Treaty forbids all nuclear testing, seismologists have redirected their attention toward the detection of nuclear explosions, regardless of size. This is a difficult task because each day there are hundreds of naturally occurring earthquakes and large non-nuclear industrial explosions associated, for example, with mining and building demolitions. It is generally possible, however, to distinguish earthquakes caused by explosions from naturally occurring earthquakes along faults. In comparison to naturally occurring earthquakes, earthquakes triggered by explosions are very shallow. Explosions occur in small spaces and, because an explosion causes the rock around it to dilate, produce strong compressional body waves that travel through the Earth. Earthquakes along faults, in contrast, are caused by slip distributed over large areas and tend to produce much larger surface waves that travel along Earth's surface. Each of these produces distinctly different seismograms and ratios of long- to short-period seismic waves. The size of an explosion can be estimated from the magnitude of the earthquake it produces. Current efforts are aimed at the identification of nuclear explosions in the 0.001 to 0.01 kiloton range, which produce earthquakes of magnitude 2 to 3.

One of the most significant events since the signing of the Comprehensive Test Ban Treaty was a series of nuclear tests conducted by India and Pakistan in May 1998. India, which was one of only three countries to oppose the treaty, conducted three nuclear tests in the northwestern part of the country. Neighboring Pakistan, which supported the treaty, but refused to sign it as long as it was opposed by India, conducted five nuclear tests in response. The tests produced earthquakes with magnitudes between 4.8 and 5.2, one of which was preceded by a naturally occurring magnitude 6.9 earthquake in Afghanistan. Seismologists have concluded that both India and Pakistan probably exaggerated the size of the tests in order to present more powerful images to each other.

The use of seismology to detect remote explosions is not limited to nuclear test monitoring. It can also be used to learn about large explosions due to other causes, especially in foreign countries or inaccessible areas. Seismologists using publicly available information, for example, were able to determine that two separate explosions occurred when the Russian submarine *Kursk* sank in August 2000. A small explosion was followed about two minutes later by a second explosion that released about 16 times as much energy as the first and produced a magnitude 4.2 earthquake that was recorded as far as 5000 km away. It was further determined that the energy released in the second explosion was equivalent to that which would have been released by 2000 to 4000 kg (about 2 to 4 kilotons) of TNT. The depth of the second explosion was estimated from a bubble pulse produced during the explosion, which was caused when a bubble of hot gas oscillates while rising quickly through the water. The calculated depth of 100 m is about the same as the seafloor depth at the location of the *Kursk* accident, so the second explosion probably occurred when the sinking submarine struck the seafloor. More than 150 earthquakes with magnitudes of 1.4 to 1.6 occurred in the months after the sinking. They were probably caused by depth charges that were detonated by the Russian navy to discourage foreign submarines from visiting the wreckage. Similar studies have shed light on incidents such as the 1995 attack on the Murrah Federal Building in Oklahoma City; the 1998 truck-bombing of the American Embassy in Nairobi, Kenya; and the September 11, 2001 terrorist attacks on the World Trade Center and Pentagon.

FURTHER READING:

PERIODICALS:

Sykes, L.R. "Four Decades of Progress in Seismic Identification Help Verify the CTBT." *Eos, Transactions, American Geophysical Union* vol. 83, no. 44 (October 29, 2002): 497, 500.

Wallace, T.C. "The May 1998 India and Pakistan Nuclear Tests." *Seismic Research Letters* vol. 69 (1998): 386–93.

ELECTRONIC:

Koper, Keith. "Seismology and Nuclear Explosions." August 21, 2002. St. Louis University. <http://mnw.eas.slu.edu/People/KKoper/EASA-130/gt;(6 December 2002).

United States Department of Energy. "Nuclear Explosion Monitoring Research & Engineering Home Page." December 5, 2002. <http://www.nemre.nn.doe.gov/nemre/>(5 December 2002).

Wallace, Terry C. "Did Iraq Test a Nuclear Weapon in 1989?" University of Arizona. <http://www.geo.arizona.edu/geophysics/faculty/wallace/IRAQ/>(5 December 2002).

———. "Forensic Seismology and the Sinking of the Kursk." University of Arizona. <http://www.geo.arizona.edu/geophysics/faculty/wallace/RUSSIANSUB/>(5 December 2002).

SEE ALSO

Clinton Administration (1993–2001), United States National Security Policy
DOE (United States Department of Energy)
Nonproliferation and National Security, United States
Nuclear Detection Devices
Nuclear Weapons
Seismograph
Seismology for Monitoring Explosions
Weapons of Mass Destruction, Detection

Senate Select Committee on Intelligence, United States

Established in the wake of congressional investigations regarding activities of United States intelligence services in the 1970s, the Senate Select Committee on Intelligence (SSCI) is, along with the House Permanent Select Committee on Intelligence, the principal means by which Congress oversees the intelligence community. In addition to reviewing, studying, and reporting on intelligence activities and programs, the SSCI is responsible for submitting to the Senate appropriate proposals for legislation.

The SSCI was created by Senate Resolution 400 in 1976, the same year that the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Frank Church (D-ID), completed its investigations of U.S. intelligence activities. Whereas the relationship of the Church Committee to the intelligence community was largely adversarial, the SSCI has developed as an entity that, while maintaining scrutiny of intelligence activities, also makes recommendations to increase the effectiveness of U.S. intelligence.

Each year, the SSCI undertakes a review of the intelligence budget submitted by the president, and prepares legislation authorizing appropriations for civilian and military agencies within the intelligence community. The SSCI also makes recommendations to the Senate Armed Services Committee regarding authorizations for intelligence activities of the military services.

During the late twentieth and early twenty-first centuries, areas of focus for the SSCI included modernization of the U.S. signals intelligence system and improving the implementation of intelligence obtained from satellites and other collection platforms. Particular areas of concern under the administration of President William J. Clinton included satellite and missile technology transfers to the People's Republic of China and Chinese efforts to influence U.S. policy.

FURTHER READING:

BOOKS:

Legislative Oversight of Intelligence Activities: The U.S. Experience: A Report. Washington, D.C.: U.S. Government Printing Office, 1994.

Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1994.* Knoxville: University of Tennessee Press, 1994.

Wittkopf, Eugene R., and James M. McCormick. *The Domestic Sources of American Foreign Policy: Insights and Evidence.* Lanham, MD: Rowman and Littefield Publishers, 1999.

ELECTRONIC:

Intelligence Laws and Regulations. Federation of American Scientists. <http://www.fas.org/irp/offdocs/laws.htm> (March 26, 2003).

Intelligence Oversight. <http://intellinet.muskingum.edu/oversight_folder/oversighttoc.html> (March 26, 2003).

U.S. Senate Select Committee on Intelligence. <http://intelligence.senate.gov/> (April 2, 2003).

SEE ALSO

Bush Administration (2001–), United States National Security Policy
Church Committee
CIA, Legal Restriction
Clinton Administration (1993–2001), United States National Security Policy
Intelligence Authorization Acts, United States Congress
Intelligence, United States Congressional Oversight

Sendero Luminoso (Shining Path, or SL)

Former university professor Abimael Guzman formed Sendero Luminoso (Shining Path, or SL) in the late 1960s,

and his teachings created the foundation of SL's militant Maoist doctrine. In the 1980s, SL became one of the most ruthless terrorist groups in the Western Hemisphere; approximately 30,000 persons have died since Shining Path took up arms in 1980. Shining Path's stated goal is to destroy existing Peruvian institutions and replace them with a communist peasant revolutionary regime. It also opposes any influence by foreign governments, as well as by other Latin American guerrilla groups, especially the Tupac Amaru Revolutionary Movement (MRTA).

In 2001 the Peruvian National Police thwarted an SL attack against "an American objective," possibly the U.S. Embassy, when they arrested two Lima SL cell members. Addtionally, government authorities continued to arrest and prosecute active SL members, including Ruller Mazombite (a.k.a. "Camarada Cayo"), chief of the protection team of SL leader Macario Ala, (a.k.a. "Artemio"), and Evorcio Ascencios (a.k.a. "Camarada Canale"), logistics chief of the Huallaga Regional Committee. Recent counterterrorist operations targeted pockets of terrorist activity in the Upper Huallaga River Valley and the Apurimac/Ene River Valley, where SL columns continued to conduct periodic attacks.

Organization Activities. The Shining Path has conducted indiscriminate bombing campaigns and selective assassinations. Shining Path adherents detonated explosives at diplomatic missions of several countries in Peru in 1990, including an attempt to car bomb the U.S. Embassy. Peruvian authorities continue operations against the Shining Path groups in the countryside, where Shining Path conducts periodic raids on villages.

Actual Shining Path membership is unknown, but is estimated by U.S. government experts to be about 200 armed militants. SL's strength has been vastly diminished by arrests and desertions. The Shining Path operates in Peru, with most activity in rural areas.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

SENTRI (Secure Electronic Network for Travelers' Rapid Inspection)

The SENTRI (Secure Electronic Network for Travelers' Rapid Inspection) is a component of the Port Passenger Accelerated Service System (PORTPASS) in use at selected border crossings (e.g., crossings at the U.S. and Mexico border in California and Texas) to facilitate quick passage through entry inspection checkpoints. SENTRI and other expedited U.S. national entry systems are designed to identify pre-approved low-risk international travelers using a combination of biometric measurements and encodable data. Automated entry systems are designed to allow inspectors additional time to focus on high-risk entrants.

SENTRI screens program participants and their vehicles against information formerly maintained in former INS and U.S. Customs Service databases. On March 1, 2003, custody of the database was assumed by the Department of Homeland Security (DHS).

SENTRI applicants are fingerprinted, and agents conduct background investigations to verify immigration status and assure the applicant has no prior criminal record. Prior to DHS reorganization, U.S. custom agents were responsible for conducting screening interviews and for conducting preliminary vehicle inspections.

SENTRI features dedicated commuter lanes at entry points . SENTRI systems utilize a combination of technologies to verify the identity of individuals in vehicles. SENTRI's dedicated commuter lanes also use a radio frequency tags affixed to the vehicle to allow moving identification of the vehicle.

When an approved SENTRI participant passes through the SENTRI system, digital license plate readers and camera scans allow inspectors to validate both the identity of the vehicle and the identity of the occupants of the vehicle against digitized photographs of approved participants in the SENTRI database and other law enforcement databases.

Initially, a system of barricades funnels traffic to an automated inspection zone where the SENTRI Automatic Vehicle (AVI) system, consisting of an in-ground inductive loop and a free-standing light curtain, scans the vehicle. The system then interrogates an RF transmitter located on the vehicle. The ensuing transmission of data primes subsequent systems for analysis and comparison of physical data and data stored in the SENTRI database. Data comparisons are also made between data encoded on a magnetic stripe on the program participant's PORTPASS identification card. Either in person or via camera, inspectors also visually compare prospective entrants against the data maintained in the SENTRI database. Lacking a positive identification, some combination of electric gates,

tire shredders, and traffic restriction barriers prevent physical passage through the entry checkpoint.

As with other automated entry systems, SENTRI utilizes a "one-to-one" search protocol to verify identity. Instead of comparing input data across a broad database, an identification number allows direct comparison with the data on file for a particular PORTPASS identification number. Biometric measurements, including fingerprints are also associated with the PORTPASS SENTRI identification number should further identity interrogation be required. Unlike fingerprint search protocols used by the FBI, the entry search protocols are, as of March 2003, unable to take biometrics and conduct a broad search to identify a subject's identity.

As of March 1, 2003, the newly created DHS absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS.

BTS is also scheduled to incorporate the United States Customs Service (previously part of the Department of Treasury).

Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the reorganization the INS formally ceases to exist on the date the last of its functions are transferred.

Although the description of the technologies involved in the SENTRI entry security program remained stable, in an effort to facilitate border security BTS plans envision higher levels of coordination between formerly separate agencies and databases. As of April 2003, the specific coordination and future of the SENTRI program was uncertain with regard to name changes, program administration, and policy changes.

■ FURTHER READING:

ELECTRONIC:

Department of Homeland Security. April 2, 2003. <http://www.dhs.gov/dhspublic/index.jsp> (April 11, 2003).

Department of Homeland Security. Secure Electronic Network for Travelers Rapid Inspection (SENTRI). March 26, 2003.<http://www.immigration.gov/graphics/shared/lawenfor/bmgmt/inspect/sentri.htm> (April 9, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <http://www.immigration.gov/graphics/shared/howdoi/inspass.htm> (April 9, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <http://www.immigration.gov/graphics/howdoi/portpass.htm> (April 9, 2003).

SEE ALSO

APIS (Advance Passenger Information System)
IBIS (Interagency Border Inspection System)
IDENT (Automated Biometric Identification System)
INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System)
NAILS (National Automated Immigration Lookout System)
PORTPASS (Port Passenger Accelerated Service System)

September 11 Terrorist Attacks on the United States

■ K. LEE LERNER

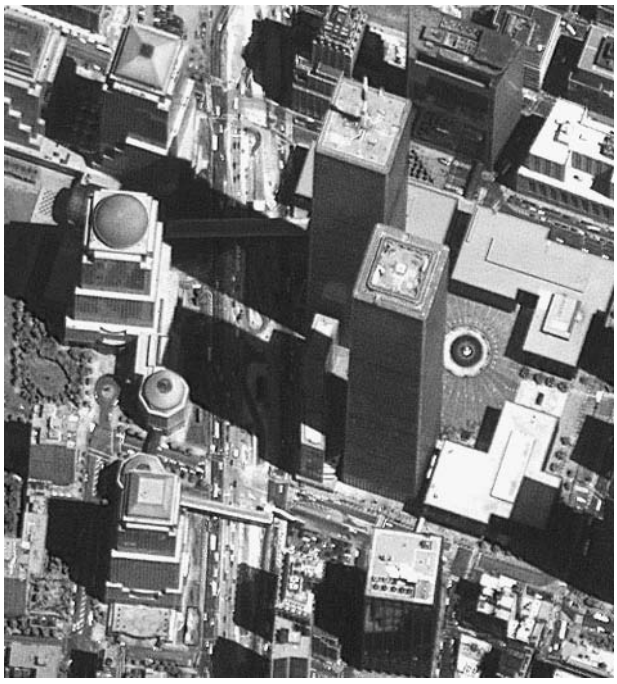
On September 11, 2001, 19 al-Qaeda-trained terrorists hijacked four U.S. commercial airliners. The hijackers crashed two of the jets into the World Trade Center towers in New York City and crashed the third jet into the Pentagon outside Washington, D.C. Passengers and crew battled the hijackers for control of the fourth jet, and it crashed into a field near Shanksville, Pennsylvania, short of reaching the hijackers' intended target in Washington, D.C.

The attacks caused the subsequent collapse of the World Trade Center twin towers, damaged the Pentagon, and killed approximately 3,000 people. Included in the death toll were hundreds of firefighters and rescue personnel who responded to the crashes at the World Trade Center site and who were in the process of rescuing those inside when the buildings collapsed.

Al-Qaeda (also known as al-Qaida), and its leader, Osama bin Laden (also spelled Usama Bin Ladin or Osama bin Ladin), subsequently claimed responsibility for the attacks. Al-Qaeda—operating out of Afghanistan under the protection of the fundamentalist Taliban regime—and allied Islamic extremist groups had publicly vowed a terrorist war against the U.S. and Western interests in an effort to establish pro-Islamist governments and fundamentalist Islamist social order throughout the world. Al-Qaeda also directed the 2000 attack on the USS *Cole* near the port of Aden, Yemen, and claimed responsibility for the bombings of U.S. embassies in Africa.

The September 11, 2001 attacks were the most deadly international terrorist attack in history and the largest attack on United States territory since the Japanese attack on Pearl Harbor on December 7, 1941.

According to investigators and transcripts of cellular phone calls made by passengers aboard several of the



Satellite views of lower Manhattan before the September 11, 2001, terrorist attacks. SPACE IMAGING.

Satellite views of lower Manhattan after the September 11, 2001, terrorist attacks. SPACE IMAGING.

hijacked planes, the hijackers used box cutter knives as weapons to overpower or kill crew and resisting passengers. The aircraft, all destined for long flights and heavy with jet fuel, exploded as powerful bombs upon impact.

The hijacking of American Airlines flight 11. The terrorist action began when five terrorists hijacked American Airlines flight 11, a Boeing 767 aircraft carrying 92 people that departed Boston bound for Los Angeles at 8:00 A.M. The FBI subsequently identified the hijackers as Satam M.A. al-Suqami (most hijackers had multiple aliases), Waleed M. al-Shehri, Wail M. al-Shehri; Mohamed Atta, and Abdulaziz Alomari. The hijackers flew American Airlines flight 11 into the North Tower of the World Trade Center in New York City at 8:46 A.M.

The hijacking of United Airlines flight 175. Five terrorists hijacked United Airlines flight 175, a Boeing 767 aircraft that departed Boston for Los Angeles at 8:14 A.M. with 65 people on board. The FBI subsequently identified the hijackers as Marwan al-Shehhi, Fayez Rashid Ahmed Hassan al-Qadi Banihammad, Ahmed Alghamdi, and Mohand al-Shehri. The hijackers piloted United Airlines flight 175 into the South Tower of the World Trade Center at 9:03 A.M., 17 minutes after the crash of American Airlines flight 11 into the North Tower.

The hijacking of American Airlines flight 77. Five terrorists hijacked American Airlines flight 77, a Boeing 757 carrying 64 people that took off from Washington Dulles Airport bound for Los Angeles at 8:21 A.M. The FBI subsequently identified the hijackers as Khalid Almihdhar, Majed Moqed, Nawaf Alhazmi, Salem Alhazmi, and Hani Hanjour. The terrorists crashed the plane into the Pentagon at 9:43 A.M. The crash into the Pentagon—exactly 60 years to the day after construction began on the building—killed more than one hundred personnel working in the building's outer rings, as well as the people aboard the aircraft. The portion of the Pentagon damaged by the crash had recently been strengthened and remodeled to heighten physical security, and Pentagon officials credit those measures with saving many lives.

The hijacking of United Airlines flight 93. Four terrorists hijacked United Airlines flight 93, a Boeing 757 carrying 44 people that took off from Newark bound for San Francisco at 8:41 A.M. The FBI subsequently identified the hijackers as Saeed Alghamdi, Ahmed Ibrahim A. Al Haznawi, Ahmed Alnami, and Ziad Samir Jarrah. Passengers, made aware of the hijackers' intentions during cell phone calls to family and authorities, attempted to overpower the hijackers. Minutes prior to the crash of the aircraft, a passenger on the flight used his cell phone to call an emergency operator in Pennsylvania to report that the plane had been hijacked and that passengers and crewmembers were planning to attempt to retake the plane. At the cost of their own lives, the passengers and crew thwarted the hijackers' plans to crash the plane into a Washington area target. At 10:07 A.M. the aircraft crashed into a field southeast of

The Pentagon on September 12, 2001, as seen in a satellite image with damage visible from the previous day's terrorist attack in the upper right. SPACE IMAGING.

Pittsburgh, Pennsylvania, killing everyone on board. Intelligence developed from subsequently captured al-Qaeda terrorists indicated that the terrorists planned to crash the plane into either the U.S. Capitol or White House.

As of May, 2003, the NTSB (National Transportation Safety Board) continues to investigate the actual September 11, 2001 airline crashes associated with the terrorist attacks.

National emergency responses. At approximately 9:30 A.M., U.S. President George W. Bush, who had been visiting a Florida elementary school, spoke briefly to reporters as the Secret Service whisked him away to the security of *Air Force One.* Bush, now aware that the crashes into the World Trade Center were deliberate, but speaking ten minutes before the crash into the Pentagon, pledged that United States would find and punish the parties responsible for crashing the hijacked aircraft into the World Trade Center towers.

Minutes later, the crash into the Pentagon put official Washington into a heightened state of alert and lockdown. The U.S. Capitol, White House, State Department, Justice Department, and World Bank were evacuated.

For the first time in aviation history the Federal Aviation Administration banned all aircraft flights in United States airspace. In a largely unheralded effort, by 12:15 P.M. the airspace over the continental United States was cleared of more than 4,500 commercial and private aircraft. Pilot and air traffic controllers managed to safely land all planes, many far from their intended destinations. The FAA ban did not reopen airspace until September 13, 2001.

During a tense afternoon and for days afterwards, U.S. military deployed anti-aircraft and anti-missile batteries around New York and Washington. Five destroyers and two aircraft carriers deployed to sea from the Naval Air Station at Norfolk to monitor and protect the U.S. East Coast. Fighter and surveillance aircraft patrolled the skies over major U.S. cites.

The collapse of the World Trade Center towers. On a typical workday, an estimated 50,000 people worked in the World Trade Center complex of six buildings. Built in the 1970s, the complex included 110 -story twin towers. Prior to September 11, 2001, the World Trade Center contained offices for more than 400 companies from more than 25 countries and hosted more than 125,000 visitors each day.

Although the full details are not yet known, forensic analysis indicated that the high temperatures of the jet fuel burning in the World Trade Center towers weakened critical supporting beams. As emergency personnel raced into the building to complete the evacuation of those stranded by the fire and to begin the long climb to attack the fire on the upper floors, at 10:05 A.M. the South tower of the World Trade Center suddenly collapsed as the upper floors pancaked into lower floors. The tower collapsed nearly vertically into the deep subfloors and subterranean ground transit station. Above ground, a billowing cloud of pulverized concrete and dust blew through several blocks of lower Manhattan. A mushroom-like plume replaced the South tower in the New York skyline. The slowly clearing air revealed an above ground pile of twisted steel and pulverized wreckage. At 10:28 A.M., the North tower of the World Trade Center collapsed with all the violence of its twin. A third World Trade Center building (the 47-story "Building 7"), damaged by the falling towers, collapsed approximately seven hours later.

Rescue efforts started immediately as surviving police, firefighters, engineers, construction workers, and other arriving emergency personnel began a determined search for colleagues and civilian survivors. Although intense rescue efforts continued for more than a week, the tremendous force of the collapsing buildings spared few of those trapped inside. The tremendous volume of falling material compacted into a tight and dense mass, providing few spaces that held the possibility of finding survivors. Death for thousands had been swift, and beyond a handful of survivors found in the first hours, no one survived the full fury of the collapse. Despite a 24-hour operation throughout the winter by large and dedicated crews, a full excavation of the site and forensic determinations of human remains would take more than half a year.

The U.S. moves to full alert. Initially unaware of the extent or origin of the attack, following the attack on the Pentagon, the U.S. military was placed on full nuclear alert. In

accordance with national security protocols and continuity of government measures, President Bush was taken by *Air Force One* to Barksdale Air Force Base in Louisiana and then to the headquarters of the U.S. Strategic Air Command at Offutt Air Force Base in Nebraska. The Secret Service did not determine that it was safe for the president to return to Washington for several hours, but President Bush reportedly asked to return to the White House as soon as possible. Arriving at 7:00 P.M., within an hour and a half the president addressed the nation and vowed to find and punish the perpetrators of the terrorist attacks.

Bush subsequently activated 50,000 National Guard and Reserve members to help with rescue efforts and security.

FEMA, EPA, and scores of federal law enforcement and investigative agencies sent disaster management teams and technical aid to the crash sites.

The FBI dedicated 7,000 of its 11,000 Special Agents and thousands of FBI support personnel to the PENTTBOM investigation. "PENTTBOM" is short for Pentagon, Twin Towers Bombing.

Investigators subsequently determined that the hijackers had been in the United States for periods ranging from a week to several years. Most entered with student or tourist visas and some of those visas had expired prior to September 11. One hijacker admitted to the U.S. to study English attended the school that admitted him. A GAO report issued in 2002 revealed that 13 of the hijackers involved in the September 11 incidents had not been interviewed by U.S. consular officials prior to the granting of visas.

Hijackers Alshehri, Atta, Alomari, Shehhi, and Jarrah were all known to have pilot training. Some of the hijackers had taken pilot training in limited aspects of flight, including training in commercial jet simulators for take-off and flight, but not for landings. Mohamed Atta was identified as the terrorist group leader.

The majority of the hijackers were Saudi nationals, Atta was an Egyptian national.

In 2002 Zacarias Moussaoui, a 34-year-old French citizen of Moroccan origin, was charged with six counts of conspiracy and faced a possible death sentence for alleged involvement in the attacks on New York and Washington. Moussaoui, indicated as the "20th hijacker" by U.S. justice officials, was unable to participate in the mission because he was already under arrest. Moussaoui has denied involvement in the attacks, but admitted to being a member of the al-Qaeda network.

The circumstances surrounding Moussaoui's arrest also sparked controversy and calls for reform with the FBI. An FBI internal investigation following the September 11 terrorist attacks revealed that Special Agent Colleen Rowley of the Minneapolis office had requested a warrant to conduct electronic surveillance and a computer search against Moussaoui well before the September 11 attacks. Rowley was suspicious of Moussaoui's activities at a local flight school that reported that Moussaoui told instructors that he was only interested in take-off and in-flight operations, but did not care to learn how to land a plane. Moussaoui was arrested for immigration violations prior to the September 11 terrorist attacks, but supervisors denied Rowley's request for a search warrant. Subsequent examination of Moussaoui's computer records revealed phone numbers used by other September 11th hijackers.

International reactions. Citizens of 90 countries perished in the terrorist attacks. There was an outpouring of sympathy from much of the world. French President Jacques Chirac was the first foreign leader to visit the World Trade Center site to express French solidarity with the American people. *Le Monde,* the leading French newspaper, ran a sympathetic headline proclaiming solidarity with Americans in their mourning. The United Kingdom lost 67 citizens in the attack, and U.K. Prime Minister Tony Blair pledged full support for the forming U.S. war on terrorism.

Not all reactions were positive; in some Arab cities there were jubilant street celebrations. Unfounded rumors and disinformation swept the Internet that Jewish citizens had mysteriously been forewarned of the attack. In fact, Israeli citizens were among the doomed hijacked passengers and other Israelis died in the World Trade Center collapses. A best-selling book in France speciously claimed that the crash into the Pentagon was a hoax.

In the wake of the September 11 attacks, the Bush administration, with the majority of Congress supporting, effectively declared war on terrorism. Casting aside diplomatic formalities, Bush reverted to the language and ethics of the American frontier when he asserted that bin Laden was wanted "dead or alive" and that, "if he can not be brought to American justice, American justice will find him."

The Old West analogies confounded many of America's European allies, but revealed a deep and fundamental shift in American foreign policy. The emerging Bush doctrine asserted that in the coming war on terrorism, "states were either for us or against us" and that "states that harbor or aid terrorists are as guilty as the terrorists themselves."

Attorney General John Ashcroft and FBI Director Robert S. Mueller, III restructured the Federal Bureau of Investigation's efforts toward counterterrorism. Congress passed and Bush signed into law the Patriot Act into law, giving the FBI and CIA broader investigatory powers and allowing them to share confidential information about suspected terrorists.

With Congressional support, Administration officials created an Office of Homeland Security and put into motion the subsequent creation of the Department of Homeland Security.

The September 11 attacks changed many aspects of American life and governmental policies. Almost every government agency reacted to the attack, changing or implementing emergency protocols and policies directed toward increased security. For example, the FAA enacted tougher airport security measures, required background checks for all airport employees with access to secure areas, and published new rules prohibiting passengers from carrying-on knives and other potential weapons. Airline and airport security reform was a key aspect of international anti-terrorist efforts. The U.S. dramatically increased air marshal protections, swelling the police force from approximately 35 officers pre-September 11 to more than a thousand officers. In addition, prior to departure of every international flight bound for the United States, APIS (Advance Passenger Information System) data is now checked against the Interagency IBIS (Interagency Border Inspection System) database. The Computer Assisted Passenger Prescreening System (CAPPS), used selectively used before September 11, came into regular use at American airports. Security screeners were place under the control of the newly created Transportation Security Administration (TSA) and airports were required to use explosive-detection devices in the inspection of passengers and baggage.

Intelligence analysts asserted that a lack of human intelligence and over-reliance on technological spying contributed to failures to develop information that might have specifically predicted the attacks. In the aftermath of the attacks, the CIA and other agencies placed a renewed emphasis on the gathering of intelligence from human sources.

FURTHER READING:

BOOKS:

Halberstam, David. *New York September 11.* New York: PowerHouse Books, 2001.

Langewiesche, William. *American Ground: Unbuilding the World Trade Center.* North Point Press, 2002.

One Nation: America Remembers September 11, 2001. Boston: Little, Brown, 2001.

PERIODICALS:

"Black September 11." *Air Force Magazine* 95, no. 9 (September 2002): 46–53.

"Responses to ASR's Survey on Aviation Security Post-Sept. 11." *Airport Security Report* 9, no. 19 (September 11, 2002): 1.

Thomas, Evan. "The Road to September 11." *Newsweek.* 138, no. 14 (October 1, 2001): 38–49.

ELECTRONIC:

"Nuclear Security—Before and after September 11." U.S. Nuclear Regulatory Commission. September 23, 2002. <http://www.nrc.gov/what-we-do/safeguards/response-911.html> (December 11, 2002).

Federal Aviation Administration. "Fact Sheet: Chronology of Events on September 11, 2001" <http://www1.faa.gov/index.cfm/apa/1064/320D8B51-A894–4E4F-AFA3B5A9A475A46D> (May 25, 2003).

U.S. Department of State. International Information Programs. "September 11, 2001. Basic Facts" August 15, 2002. <http://usinfo.state.gov/topical/pol/terror/020815basic.htm> (May 25, 2003).

U.S. Department of State. "Patterns of Global Terrorism, 2001. <http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10235.htm> (May 25, 2003).

The White House. September 11, 2001. "Statement by the President in His Address to the Nation" <http://www.whitehouse.gov/news/releases/2001/09/20010911–16.html#> (May 25, 2003).

SEE ALSO

Air Marshals, United States
Airline Security
Al-Qaeda (also known as Al-Qaida)
CIA (United States Central Intelligence Agency)
Disinformation
FAA (United States Federal Aviation Administration)
FBI (United States Federal Bureau of Investigation)
FEMA (United States Federal Emergency Management Agency)
Iraqi Freedom, Operation (2003 War Against Iraq)
Homeland Security, United States Department
NTSB (National Transportation Safety Board)
World Trade Center, 1993 Terrorist Attack
World Trade Center, 2001 Terrorist Attack

Sequencing

BRIAN HOYLE

Sequencing refers to the techniques used to determine the order of the constituent bases (i.e., adenine, thymine, guanine, and cytosine) of deoxyribonucleic acid (DNA) or protein. Protein sequencing determines the order of the constituent amino acids. Sequencing is increasingly important in forensic science and in the rapid and positive identification of potential pathogens that can be exploited by bioterrorists.

DNA is typically sequenced for several reasons: to determine the sequence of the protein encoded by the DNA, the location of sites at which restriction enzymes can cut the DNA, the location of DNA sequence elements that regulate the production of messenger RNA, or alterations in the DNA.

The sequencing of DNA is accomplished by stopping the lengthening of a DNA chain at a known base and at a known location in the DNA. Practically, this can be done in two ways. In the first method, called the Sanger-Coulson procedure, a small amount of a specific so-called

dideoxynucleoside base is incorporated in along with a mixture of the other four normal bases. This base is slightly different from the normal base and is radioactively labeled. The radioactive base becomes incorporated into the growing DNA chain instead of the normal base, growth of the DNA stops. This stoppage is done four times, each time using one of the four different dideoxynucleosides. This generates four collections of DNA molecule. Also, because replication of the DNA always begins at the same point, and because the amount of altered base added is low, for each reaction many DNA pieces of different length will be generated. When the sample is used for gel electrophoresis, the different sized pieces can be resolved as radioactive bands in the gel. Then, with the location of the bases known, the sequence of the DNA can be deduced. The second DNA sequencing technique is known as the Maxam-Gilbert technique, after its co-discoverers. In this technique, both strands of double-stranded DNA are radioactively labeled using radioactive phosphorus. Upon heating, the DNA strands separate and can be physically distinguished from each other, as one strand is heavier than the other. Both strands are then cut up using specific enzymes, and the different sized fragments of DNA are separated by gel electrophoresis. Based on the pattern of fragments the DNA sequence is determined.

The Sanger-Coulsom is the more popular method. Various modifications have been developed and it has been automated for very large-scale sequencing. During the sequencing of the human genome, a sequencing method called shotgun sequencing was very successfully employed. Shotgun sequencing refers to a method that uses enzymes to cut DNA into hundreds or thousands of random bits. So many fragments are necessary since automated sequencing machines can only decipher relatively short fragments of DNA about 500 bases long. The many sequences are then pieced back together using computers to generate the entire DNA genome sequence.

Protein sequencing involves determining the arrangement of the amino acid building blocks of the protein. It is common to sequence a protein by the DNA sequence encoding the protein. This, however, is only possible if a cloned gene is available. It still is often the case that chemical protein sequencing, as described subsequently, must be performed in order to manufacture an oligonucleotide probe that can then be used to locate the target gene. The most popular direct protein chemical sequencing technique in use today is the Edman degradation procedure. This is a series of chemical reactions, that remove one amino acid at a time from a certain end of the protein (the amino terminus). Each amino acid that is released has been chemically modified in the release reaction, allowing the released product to be detected using a technique called reverse phase chromatography. The identity of the released amino acids is sequentially determined, producing the amino acid sequence of the protein.

Another protein sequencing technique is called fast atom bombardment mass spectrometry, or FAB-MS. This is a powerful technique in which the sample is bombarded with a stream of fast atoms, such as argon. The protein becomes charged and fragmented in a sequence-specific manner. The fragments can be detected and their identify determined. The expense and relative scarcity of the necessary equipment can be a limitation to the technique.

Still another protein sequencing strategy is the digestion of the protein with specialized protein-degrading enzymes called proteases. The shorter fragments that are generated, called peptides, can then be sequenced. The problem then is to order the peptides. This is done by the use of two proteases that cut the protein at different points, generating overlapping peptides. The peptides are separated and sequenced, and the patterns of overlap and the resulting protein sequence can be deduced.

FURTHER READING:

BOOKS:

Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction.* Washington, DC: Carnegie Endowment for International Peace, 2002.

PERIODICALS:

Balding D. J. "The DNA Database Search Controversy." *Biometrics* 2002 Mar; 58(1): 241–4.

Henderson J. P. "The Use of DNA Statistics in Criminal Trials." *Forensic Sci Int.* 2002 Aug 28; 128(3): 183–6.

Mullis, K. B. and F. A. Faloona."Specific Synthesis of DNA in vitro via a Polymerase catalysed Chain Reaction." *Methods in Enzymology* no. 155 (1987): 335–50.

SEE ALSO

Anthrax Weaponization
Biological Weapons, Genetic Identification
Genetic Information: Ethics, Privacy and Security Issues
Genetic Technology
Genomics
Infectious Disease, Threats to Security

Serbia, Intelligence and Security

Following the dissolution of Yugoslavia in 1989, after the fall of Soviet communism in Eastern Europe, the Balkan region fell into conflict. The former Yugoslav provinces splintered into several independent nations, but Serbia and Montenegro chose to remain a communist dominated state. The Federal Republic of Yugoslavia, as the nation was renamed, is wholly dominated by Serbia.

When civil war erupted in neighboring Bosnia-Herzegovina, Serbia provided aid to ethnic Serb forces in the region. The international community protested the move, and Yugoslav leader, Slobidan Milosevic signed a peace accord with neighboring Bosnia and Croatia. In 1999, Serbia refused to restore autonomy to Kosovo. Conflict lingered, and reports that Serbian forces were perpetrating grievous human rights crimes against Muslim Kosavars, including mass murder and deportation, prompted NATO intervention in the region. Following a bombing campaign against Serbian strongholds, peacekeeping troops entered the region.

Following the Kosovo conflict, Serbians ousted Milosevic in a general election. Vojislav Kostunica was the first non-communist leader elected in Yugoslavia in nearly 60 years. Though tension remains high in the region, and periodic violence continues to erupt, Kostunica and his government are committed to democratizing the national government and reforming the economy. The function of the national intelligence community has changed dramatically because of reforms.

The Serbian intelligence community maintains traditional distinctions between internal and foreign, civilian and military intelligence, and organizes its various agencies accordingly. However, many of these agencies' expressed duties overlap. To avoid confusion and facilitate cooperating and data sharing, the Council for Security coordinates all intelligence and security operations relating to the protection of national interests.

Though individual branches of the military maintain their own intelligence units, the Ministry of Defense oversees the largest military intelligence agencies and coordinates the intelligence and security operations of various departments and units. The *Kontraobavesajna Sluzba* (KOS), General Staff Security Directorate, provides domestic security and counterintelligence analysis for the military. The agency works closely with Military Police to insure the safety and security of Serbian military installations.

Civilian intelligence forces fall under the jurisdiction of the Ministry of the Interior. The *Sluzba Javne Bezbednosti* (SJB), Public Security Service is charged with the protection of public welfare. The SJB guards diplomatic officials and aids intelligence services with anti-terrorism operations. The future of this organization, as well as its parent, the State Security Service (SDB), is unknown. Government officials have reformed the organization several times, stripping it of its powers to conduct espionage for political reasons.

In 2000 the government created a special anti-terrorist unit, the ATJ. The group is trained in both civilian espionage and military battle techniques. The special unit was granted a wide range of operation, from intelligence to policing.

The structure of the Yugoslavian intelligence community is sure to change in the near future, as the government continues reforms. Serbian intelligence and security agencies have cultivated a regional reputation for brutality over the past six decades, a problem that democratic reformers seek to rectify. The new government arrested Milosevic and sent him to stand trial for war crimes and crimes against humanity. The international tribunal convicted Milosevic. Since the elections of Kostunica and Prime Minister Zoran Djindjic, the nation has made strides to join the international community and participate in European economic and security organizations.

On March 12, 2003, Djindjic, one of the primary leaders of Serbia's reform movement, was assassinated by an unknown sniper.

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union
European Union

Sex-for-Secrets Scandal

▮ DAVID TULLOCH

On December 14, 1986, a United States Marine who had been serving as an Embassy guard in Moscow and Vienna turned himself in to CIA officials. The Marine, Sergeant Clayton J. Lonetree, claimed that he had given classified information to a KGB agent with the codename "Uncle Sasha." Immediately, a government investigation was launched into the affair, as officials searched for evidence that Lonetree had not been working alone, or was just one of many Embassy guards who was successfully targeted by the Soviets.

Violetta and 'Uncle Sasha.' Lonetree, a Winnebago Indian from St. Paul, Minnesota, had been a model soldier. He enlisted at age eighteen in the Marine Corps, and later underwent the difficult, elite training of the Security Guard Battalion School, from which he graduated in 1984. Lonetree was then assigned to the U.S. Embassy in Moscow, and later to the Vienna Embassy. While everyday duty as an Embassy guard can be repetitive, it is a key position, and often includes access to sensitive material, such as keys to offices or safes.

It was while stationed in Moscow that Lonetree met Violetta Sanni (sometimes given as Seina), a local Russian who worked as a translator, while attending the annual Marine ball held at the Ambassador's residence in November 1985. Lonetree began to date Violetta, despite the Marine Corps prohibition against guards having close contacts with Soviet citizens, and he seems to have fallen in love with her. Sanni then introduced Lonetree to "Uncle

Christine Keeler, a call girl involved with British War Minister Lord John Profumo in a 1963 "sex for secrets" scandal, was also entangled with a Soviet spy trying to discover British nuclear secrets. ©BETTMANN/CORBIS.

Sasha," later identified as Alexi Yelsimov. At first Lonetree enjoyed the visits of Sasha, and they talked together about Lonetree's home, what his life had been like in the United States and on various political topics. However, Sasha was a KGB operative and he began to ask Lonetree questions.

Despite his concern, Lonetree continued to see Violetta and befriend Sasha, without notifying his superiors until the end of his Moscow tour. He was reassigned to the Vienna Embassy, where he was unexpectedly joined by Uncle Sasha. The KGB agent became Lonetree's only contact with Violetta, giving the lonely soldier photos and packages from Moscow, and passing on Lonetree's letters and gifts. Sasha used this new position as go-between to persuade Lonetree to provide documents and information from the embassy. Lonetree admitted to giving Sasha an old embassy phonebook and floor plans, for which he was paid $1,800. The Marine also provided details on suspected intelligence agents working undercover in the embassy.

Confession and conviction. Uncle Sasha began to demand more information from Lonetree, even suggesting a trip to Moscow for KGB training and to see Violetta again. Lonetree decided he had had enough, and turned himself in to the CIA. Nine months of intensive investigations began by the Naval Criminal Investigative Service (NCIS) and other agencies, which led to an additional five other Marine guards being detained on suspicion of espionage, lying to investigators, and improper fraternization with foreign nationals.

One of these detainees was Corporal Arnold Bracy, who was also suspected of having a romantic liaison with a Soviet woman and being an accomplice of Lonetree's. Bracy signed a confession that stated he had helped commit a number of serious breaches of security. Bracy later claimed not to have read the document before signing it and to have signed under duress. A key claim in the confession was that Bracey and Lonetree had worked together to facilitate tours of the Moscow Embassy for KGB agents and allow them to plant listening devices. This allegation was denied by both Bracy and Lonetree, and it became evident that, working together, it would have been difficult for the two soldiers to show KGB agents through the embassy without being detected by other guards or electronic security measures. Eventually, all charges against Bracy were dropped. However, Lonetree was convicted on all of the thirteen charges he faced, becoming the first U.S. Marine to be found guilty of espionage.

Doubts surface. Lonetree was sentenced to 30 years in prison in November 1987 as well as a reduction in rank to private, the loss of all military pay and privileges, a $5000 dollar fine, and a dishonorable discharge. Even so, some doubts were raised about the NIS investigation, as a number of the accusations leveled against Lonetree, Bracy, and others were later shown to be unfounded.

In 1991, Lonetree returned to court asking that his conviction be overturned. In the U.S. Court of Military Appeals, lawyers claimed that Lonetree's confession had been inappropriately used as evidence against him, as it had been taken on the understanding that it would remain confidential. It was also suggested that Lonetree's lawyers at his original trial had been incompetent, as they had not informed their client of the possibility of a plea agreement. Additionally, they argued that Lonetree's cooperation should have earned him a drastically reduced sentence.

During Lonetree's trial, it was noted that one witness had remained anonymous, which was a violation of the defendants basic right "to know the identity of the witness against him." The witness, a CIA agent, had mostly testified in closed session. As well, military courts have procedures that differ from civil courts. At one time, it was even claimed that Lonetree had purposefully only given the KGB non-vital information, as he was planning to become a double agent.

While Lonetree's thirty-year sentence was not overturned, the court did agree that it should be reduced. In May 1988 the term had been shortened by five years for

the cooperation he had shown investigators. Then in October 1992 another five years reduction was given. After the unsuccessful appeal, yet another shortening of five years' was granted in July 1994. In 1996, after serving just under nine years in jail, Lonetree was released early for good behavior.

The material that Lonetree passed to the KGB was not considered of great significance, and one report suggested the security implications were probably minimal. However, by coming forward, Lonetree revealed significant security lapses within the embassy staff structure that sparked changes in procedures and improved security in embassies across the world.

FURTHER READING:

BOOKS:

Barker, Rodney. *Dancing with the Devil: Sex, Espionage, and the U.S. Marines—The Clayton Lonetree Story.* New York: Simon & Schuster, 1996.

Headley, Lake, and William Hoffmann. *The Court Martial of Clayton Lonetree.* New York: Henry Holt, 1989.

Kessler, Ronald. *Moscow Station: How the KGB Penetrated the American Embassy.* New York: Scribner's, 1989.

SEE ALSO

Cold War (1972–1989): The Collapse of the Soviet Union
Navy Criminal Investigative Service (NCIS)
Reagan Administration (1981–1989), United States National Security Policy

Ships Designed for Intelligence Collection

JUDSON KNIGHT

The concept of using ships as modern intelligence-gathering platforms evolved, along with larger modern ideas of intelligence operations in general, from World War II. The Cold War saw the deployment, on both the Soviet and American sides, of ships tasked with gathering communications and electronic intelligence. Some of these were disguised as fishing vessels, a practice common on the Soviet side, while the United States favored vessels operating under the guise of research craft. During the 1960s, United States ships designed for intelligence collection figured in a number of unfortunate incidents that contributed to the end of the seaborne passive electronic intelligence (ELINT) program.

The Soviet Union. Due to their relative lack of electronic listening posts overseas—in comparison to the Americans, who possessed signals intelligence (SIGINT) facilities throughout the world—the Soviets initially took the lead in the use of ships to gather intelligence. From the 1950s, they began using what came to be their preferred intelligence-gathering craft, a fishing trawler. The design of the trawler, which was made to store many days' catch in insulated compartments, made it ideal for extensive activities below deck.

As the Cold War continued, the Soviets expanded and improved their intelligence-collection ships, known to U.S. intelligence as AGIs, the *AG* being code for "miscellaneous auxiliary" and the *I* a designator of enemy craft. Later models were designed and built specifically to serve as collection platforms. Eventually they became large enough to include on-board intelligence processing facilities, greatly improving the speed with which raw data became usable intelligence for Soviet operatives.

During the Vietnam War, a pair of Soviet AGIs, one near Guam and the other in Vietnam's Gulf of Tonkin, kept a close watch on U.S. forces, and in some cases may have provided Hanoi with advance notice of U.S. airstrikes. Near the end of the Cold War, the Soviets had a fleet of about five dozen AGIs dispatched throughout the globe. A particular area of interest lay just to the east of Florida, in international waters and close to friendly ports in Cuba, from which Soviet AGIs could monitor activities at U.S. naval bases in South Carolina, Georgia, and Florida.

The United States. Among the few places where the United States, like the Soviet Union, lacked sufficient electronic listening posts were South America and Africa, to which the first U.S. spy ships were deployed in the early 1960s. Most such craft were cargo ships from World War II, converted by the National Security Agency (NSA) into craft for gathering SIGINT, particularly ELINT. Ships in this first phase of the U.S. maritime intelligence-gathering effort were designated T-AG, or civilian miscellaneous auxiliary craft.

Simultaneous with the T-AG phase was that of AGTR, or technical research craft. The U.S. Navy and Marines, in collaboration with NSA, operated these craft, which NSA had also converted from war-era cargo ships that had been converted. The first AGTR, *Oxford,* provided information on movement of Soviet arms into Cuba in the build-up toward the missile crisis of 1962.

ELINT ships in history. Of the five AGTR craft, the best was the *Liberty,* which in June 1967 was off the coast of the Sinai Peninsula. During the Six-Day War, Israeli air and naval craft, mistaking it for an enemy ship, attacked and sank it, killing 34 men and wounding 171 more. Israel later apologized and paid damages to the families of those

killed. A dozen studies by U.S. and Israeli authorities each concluded that the regrettable incident was simply a result of confusion in the midst of heavy fighting.

Two other intelligence-gathering craft also figured in well-known events. One of these was the destroyer *Maddox,* part of an ELINT-gathering mission known as DESOTO, conducted in the Gulf of Tonkin in 1964. (The *Maddox,* operating openly as a naval vessel, was not part of the AG series.) After North Vietnamese gunboats fired on it on August 4, Congress hastily passed the Tonkin Gulf Resolution, which greatly increased the scope of U.S. involvement in Vietnam.

In the meantime, the Navy and NSA, taking a page from the Soviets' book, developed the AGER (environmental research) series, using trawler-based designs for craft smaller than AGTRs. The second of three AGER craft was the *Pueblo,* captured by the North Koreans in January 1968. The *Pueblo* incident, coming as it did on the heels of the *Liberty* tragedy, brought an end to the large-scale U.S. deployment of maritime intelligence-gathering ships equipped with passive ELINT capabilities.

■ FURTHER READING:

BOOKS:

Holmes, W. J. *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During World War II.* Annapolis, MD: Naval Institute Press, 1979.

Packard, Wyman H. *A Century of U.S. Naval Intelligence.* Washington, D.C.: Naval Historical Center, 1996.

Parker, James E. *Codename Mule: Fighting the Secret War in Laos for the CIA.* Annapolis, MD: Naval Institute Press, 1995.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

Tourison, Sedgwick D. *Secret Army, Secret War: Washington's Tragic Spy Operation in North Vietnam.* Annapolis, MD: Naval Institute Press, 1995.

SEE ALSO

Intelligence
NMIC (National Maritime Intelligence Center)
Pueblo Incident
SIGINT (Signals intelligence)
Undersea Espionage: Nuclear vs. Fast Attack Subs
USS Liberty
Vietnam War

"Shoe Bomber"

On December 22, 2001, al-Qaeda sympathizer Richard Reid attempted the mid-flight destruction of an American Airlines aircraft bound from Paris to Miami flight with 197 people on board. Reid attempted to destroy the flight with plastic explosives concealed in his shoes that were capable of blowing a hole in the plane's pressurized fuselage. Passengers and crew subdued Reid after the smell of burned matches alerted them to Reid's failed attempts to light his shoes.

Authorities at the Charles de Gaulle airport in Paris had failed to check Reid's shoes—not a common pre-flight security practice at the time. Subsequent to Reid's attempt, the checking of shoes and more extensive checks for explosive residues became part of pre-flight security examinations.

Charles de Gaulle (CDG) airport had an established reputation as a "soft" entry point for terrorists. In an unrelated case occurring the year after Reid's arrest, an Algerian-born CDG baggage handler who had worked at the airport for more than three years—and who had broad access to secure areas—was arrested after weapons and explosive devices (an automatic handgun, a machine gun, five bars of plastic explosives, and two detonators) were discovered in the trunk of his car.

Prosecutors subsequently asserted that "Reid's intentions were clear he wanted to murder innocent people in the name of his fanatical religious beliefs." Reid subsequently confessed and admitted guilt to eight felony charges, including attempted murder, attempted murder using a weapon of mass destruction, planting an explosive device on an aircraft, attempted destruction of an aircraft, and two counts of interfering with a flight crew.

Reid, son of an English mother and Jamaican father, was a British citizen with a history of petty crime. He converted to radical Islam while in a British jail. Reid claimed he was an enemy of the United States, and avowed his allegiance to al-Qaeda leader Osama bin Laden.

References to an al-Qaeda operative with a similar operational history and profile to Reid were found on a computer hard drive allegedly used by al-Qaeda leaders in Afghanistan.

Reid attempted to claim he was a "solider" in the war on terrorism. At Reid's sentencing, U.S. federal judge William Young dismissed his assertions and, citing Reid's attempts to kill innocent civilians, flatly told Reid, "You are not a soldier, you are a terrorist." Reid was sentenced to life in prison without the possibility of parole.

■ FURTHER READING:

PERIODICALS:

Ferdinand, P. "Would-Be Shoe Bomber Gets Life Term." *Washington Post.* January 31, 2003; A1.

SEE ALSO

Airline Security

Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets
Terrorist Threat Integration Center

Shoe Transmitter

A popular weekly situation comedy called "Get Smart" ran on the American Broadcasting Corporation television network in the United States for five seasons in the 1960s. In the show—a spoof of spies and espionage organizations—the lead character, Maxwell Smart, often communicated with his colleagues via a "shoe phone." The television series and the espionage equipment were conceived as a nonsensical spoof of the spy movies that were in vogue at that time. Nonetheless, the shoe phone was grounded in reality.

During the Cold War, with tensions arising between the United States and the former Soviet Union in the 1950s and 1960s, both nations conducted espionage campaigns to collect information from the other country that was deemed vital to national security. As part of these efforts, the Soviet spy agency known as the KGB (Komitet Gosudarstvennoi Bezopasnosti, which translates as the Committee for State Security) devised a microphone and transmitter that could be concealed in a shoe.

The shoe transmitter could detect conversation in the immediate vicinity and broadcast the conversation to a receiver located in a nearby secret monitoring station. Essentially, the shoe transmitter was a tiny radio station, broadcasting on a frequency that would be detected only by the special receiver.

The shoe transmitter was intended to eavesdrop on conversations of someone who could supply important and privileged information. A pair of dress shoes designed to be worn for business purposes—one of which contained the microphone and transmitter in a hollow heel—was planted in the home, hotel room, or office of the subject. This was done by someone affiliated with the KGB who had ready access to the subject such as a maid, valet, or co-worker. When the shoes were planted, a pin located in a hollowed-out heel was pulled out. This activated the radio beacon and the microphone, allowing conversation to be recorded until the batteries that powered the equipment ran out of power.

With the coming of more sophisticated bugging technologies in the 1970s, the use of the shoe transmitter was phased out. However, at the time the, device was a sophisticated piece of equipment and demonstrated that miniaturization of electronic hardware was possible.

Unlike its comedic counterpart, the device could not be used to make telephone calls.

A shoe with an imbedded heel transmitter produced by the KGB during the Cold War to monitor secret conversations. ©AFP/CORBIS.

A copy of the shoe transmitter is now on display at the International Spy Museum. The museum opened in July 2002 in Washington, D.C.

FURTHER READING:

ELECTRONIC:

International Spy Museum. "Collections Overview." <http://www.spymuseum.org/media/collections.html>(20 December 2002).

SEE ALSO

Audio Amplifiers
Bugs (Microphones) and Bug Detectors
Parabolic Microphones

Short-Wave Transmitters

Short-wave radio transmission and reception occurs in the range somewhere between 2 and 30 MHz (megahertz, or million cycles per second). Because these signals are capable of propagating over a greater distance than either AM or FM radio, shortwave is the preferred medium for radio broadcasting to remote locations. World powers in the twentieth century and beyond made use of short-wave radio transmissions to bridge political and physical barriers in sending propaganda messages to distant populations.

Despite their name, shortwaves are relatively long in wavelength compared to most of the electromagnetic spectrum. They measure anywhere from 33 to 262 feet (10–80 m), gargantuan in comparison to ultra high-energy waves such as x rays and gamma rays, of which it would take many millions to cover even the length of a millimeter. On the electromagnetic spectrum, the higher the energy level, the higher the frequency, and the shorter the wavelength.

Shortwaves shorter than AM (amplitude modulation) radio waves, to which the U.S. Federal Communications Commission has assigned the frequency range of 535 kHz to 1.7 MHz. Short-wave transmissions occur somewhere between 2 to 5.9 MHz at the low end, and 26.1 to 30 MHz at the high end. Above these are microwave regions assigned to television stations, as well as FM, which occupies the range from 88 to 108 MHz. Like AM signals, those of short-wave radio transmissions propagate over a great distance because they bounce off of a heavily charged layer in the earth's ionosphere.

The length of signal propagation prompted the establishment of international short-wave communications in the late 1930s. During the Cold War, the world's major powers used shortwave to transmit propaganda messages. Examples of these efforts included the short-wave stations operated by Voice of America, Radio Moscow, Radio Beijing, and the British Broadcasting Corporation.

Long before the 2003 invasion of Iraq, the United States, through its Central Intelligence Agency, supported Iraqi short-wave stations operated by resistance movements. In June 1996, President William J. Clinton provided $6 million to the Iraqi National Accord, which set up several stations, including Twin Rivers Radio, Radio Tikrit, and al Mustaqbal. The latter, whose name means "The Future," broadcast from Kuwait and from U.S. military EC-130 psychological operations planes, on the frequency of 1575.3 kHz (1.5753 MHz), which in the United States would be a high-frequency AM station.

■ FURTHER READING:

BOOKS:

Helms, Harry L. *Shortwave Listening Guidebook: The Complete Guide to Hearing the World.* Solana Beach, CA: High Text Publications, 1993.

McCormick, Anita Louise. *Shortwave Radio Listening for Beginners.* Blue Ridge Summit, PA: TAB Books, 1993.

Yoder, Andrew R., and Hank Bennett. *The Complete Shortwave Listener's Handbook.* New York: McGraw-Hill, 1997.

ELECTRONIC:

Clandestine Radio.com. <http://www.clandestineradio.com> (April 2, 2003).

SEE ALSO

CIA, Foreign Broadcast Information Service
Electromagnetic Spectrum
National Telecommunications Information Administration, and Security for the Radio Frequency Spectrum, United States
Propaganda, Uses and Psychology

Shredding.

SEE *Document Destruction.*

SIGINT (Signals Intelligence)

■ JUDSON KNIGHT

Signals intelligence, or SIGINT, is one of the four major forms of intelligence, along with human, imagery, and measurement and signatures intelligence (HUMINT, IMINT, and MASINT respectively). As its name suggests, it is intelligence derived from the interception of signals, including communications signals, electronic emissions, and telemetry. The two major subsets of SIGINT are COMINT, or communications intelligence, gained through the interception of foreign communications (excluding open radio and television broadcasts); and ELINT or electronics intelligence, derived from the interception of non-communication electromagnetic signals, most notably radar.

Communications intercepts may be in the form of voice transmissions via telephone or radio, Morse code, teletype, or facsimile machine. In the modern intelligence environment, most such communications are encrypted, and typically require sophisticated computer technology for decryption. A major component of efforts by the intelligence services of the English-speaking world is Echelon, a worldwide system of satellites, interception stations, and supercomputers jointly operated by the United States, United Kingdom, Canada, Australia, and New Zealand. The U.S. National Security Agency (NSA) takes the lead in this and many other COMINT efforts.

Early U.S. efforts in SIGINT would today be placed under the heading of COMINT. Although the U.S. Army conducted cryptography and cryptanalysis prior to 1930, concerted efforts began in that year with the establishment of the U.S. Army Signal Intelligence Service (SIS), which consolidated all such operations. Notable activities of SIS included the breaking of the Japanese Foreign Ministry PURPLE cipher prior to World War II. SIS, renamed several times during the war, was replaced in 1945 by the Army Security Agency (ASA). In 1977, the Army Intelligence and Security Command (INSCOM) replaced

ASA. The Navy had its own COMINT activities, later taken over by NSA.

ELINT. All intercepts of non-communication signals sent over electromagnetic waves, excluding those from atomic detonations (which are the province of MASINT operations), fall under the heading of ELINT. In World War II, the Allies conducted ELINT operations involving Axis air defense radar systems, to neutralize these in a bombing raid, either through a direct hit or by electronic countermeasures. Since that time, the United States has targeted or monitored the radar operations of numerous enemies, including the Soviet Union and China during the Cold War, North Vietnam during the war in Southeast Asia, and Libya and Iran during latter-day conflicts in the Middle East.

The radar component of ELINT is not to be confused with RADINT, or radar intelligence from nonimaging radar. Unlike ELINT, RADINT does not involve the interception or radar signals; instead, intelligence regarding flight path and other specifics is derived from the deflection of enemy radar signals. RADINT is a subcategory of MASINT.

FISINT and TELINT. Actual varieties of ELINT include FISINT, or foreign instrumentation signals intelligence, and its subcategory, TELINT, or telemetry intelligence. The signals sent by foreign entities when testing and deploying aerospace, surface, and sub-surface systems—examples include tracking and aiming signals, as well as video data links—are the material of FISINT operations.

Telemetry is the process of making measurements from a remote location and transmitting those measurements to receiving equipment. It has extensive civilian and military applications. As an example of the former, an electric company may use radio signals from remote power lines to relay operational information to the center of the power grid. Among the military applications of telemetry is the use of signals to relay information on the performance of a guided missile system.

FURTHER READING:

BOOKS:

Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence.* Woodstock, NY: Overlook Press, 2002.

Alvarez, David J. *Allied and Axis Signals Intelligence in World War II.* Portland, OR: F. Cass, 1999.

Andrew, Christopher M. *Codebreaking and Signals Intelligence.* Totowa, NJ: F. Cass, 1986.

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Gilbert, James L., and John Patrick Finnegan. *U.S. Army Signals Intelligence in World War II: A Documentary History.* Washington, D.C.: U.S. Government Printing Office, 1993.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

Sexton, Donal J. *Signals Intelligence in World War II: A Research Guide.* Westport, CT: Greenwood Press, 1996.

West, Nigel. *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman.* New York: W. Morrow, 1988.

SEE ALSO

COMINT (Communications Intelligence)
Echelon
Electronic Countermeasures
HUMINT (Human Intelligence)
IMINT (Imagery Intelligence)
Intelligence
Measurement and Signatures Intelligence (MASINT)
NSA (United States National Security Agency)
Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom
Telemetry

Silencers

CARYN E. NEUMANN

A silencer is an effort to suppress sound by means of an attachment to a firearm. Generally, a six- to twenty-inch steel, titanium, or aluminum alloy barrel addition designed to work with a particular weapon, silencers have also been constructed from other materials such as plastic soft drink bottles. Nicknamed "whispering death," these devices give a shooter the ability to strike a target with less risk of being noticed. Contrary to popular image, silencers do not completely muffle the sound of a gun, but instead lessen muzzle flash, reduce muzzle noise, and decrease recoil by delaying the escape of gases from the barrel of the firearm. Generally illegal for individuals to own in most parts of the world, silencers have enjoyed enormous popularity with espionage and security forces.

The idea of a silencer is an old one, with gunsmiths experimenting with various designs to silence weapons since the nineteenth century. The first man to successfully develop and market a silencer was Hiram P. Maxim, the son of the similarly named inventor of the machine gun. In 1908, Maxim developed a silencer that delayed the release of gases, but he did not market the weapon until making a few improvements. The Maxim Model 1909, released in the year of its name, became the first efficient silencer to be marketed, but the Maxim Model 1910 became the most widely distributed silencer in the United States by capitalizing on an off-center design that allowed it to be used with

A Hungarian soldier fires an AK-47 style assault rifle equipped with a silencer. ©LEIF SKOOGFORS/CORBIS.

a weapon's original sights. Although the military value of silencers quickly became apparent to many observers, Maxim only had the goal of eliminating noise pollution. Many of the first buyers of silencers employed them for target shooting in basements and backyards so the sound of firing would not disturb others. Silencers also found a market in pest control. Many silencers are still sold for use in eliminating rats, not so much to surprise the rodents, but to avoid the public relations problems associated with shots fired in heavily occupied areas.

Despite global marketing by Maxim, no nation's military force made widespread use of silencers until World War II. The Maxim Model 1912 was the first mass-marketed silencer designed specifically for military purposes. Created for use with the popular Springfield rifle, the report of the weapon was reduced, but the sonic boom of the bullet could not be diminished. The passage of the bullet sounded like someone tearing a sheet until the projectile passed a solid object, like a tree, which resulted in the emission of a large crack. The 1912 model was not sold to any government in great numbers, perhaps because of the notorious conservativeness of military planners in this era, but it did find a few buyers. The U.S. Army purchased a few of the weapons to be used by sharpshooters for the quiet, long-range killing of sentries so that surprise attacks could be mounted. The silencers were apparently used in Mexico in the campaign against Pancho Villa, but, because the Army failed to halt Villa, the effectiveness of the silencers is somewhat in doubt. In World War I, Maxim manufactured silencers in calibers ranging from .22 through those large enough for machine guns. An experimental model silenced a four-inch artillery piece. Snipers continued to be the major users of silencers, though, and these men used only rifles. The Germans experimented with a silencer-equipped Luger pistol, but the gun suffered mechanical failure as well as too high a noise rate. In the years after the war, public interest in silencers waned, and Maxim halted production in 1925.

In the years between the World Wars, silencers failed to find a substantial market among any of the world's military forces. The U.S. military conducted a number of trials with silencers, but ultimately decided that the weapons were unfit for combat use. Despite the silenced discharge, the substantial noise created by the movement of gun parts enabled observers to easily locate the bulky weapons. While unsuitable for normal military usage, silencers appealed to intelligence agencies and these organizations continued to experiment with the weapons. The United States Office of Strategic Services (OSS), newly formed to help fight World War II, modified the Thompson submachine gun with a silencer built by the Chrysler Corporation. The gun proved too noisy to be suitable for a

silencer as well as very susceptible to jamming under field conditions. The OSS preferred to equip its agents with a silenced version of the M3 submachine gun in addition to a .30 caliber M1 carbine. The Central Intelligence Agency, successor to the OSS, used a silenced High Standard HD military pistol. Francis Gary Powers, pilot of the U-2 reconnaissance plane shot down over the Soviet Union in 1960, carried the silenced HD when he was captured. Around the world, the Welrod became a weapon of first choice. One of the few silencers designed specifically for silent and secret operations, the British-built gun was produced in .32 ACP, 9mm, and .45 ACP calibers.

When firing a standard weapon, some sort of ear protection must be utilized or temporary loss of hearing will result. Plugs and earmuffs reduce noise level, but also make it much more difficult to hear movement. Silencers make it much easier to locate and fire upon multiple targets, and this factor explains the expanding popularity of the weapons. After World War II, silencers were increasingly used in combat conditions. A silencer confuses the person being fired upon, improves the shooter's accuracy by suppressing disconcerting flash, noise, and recoil and, lastly, gives the shooter a feeling of confidence that he will not be discovered. The M3A1, an improved M3, became popular in various global hotspots like Greece, Africa, Palestine, and South America because the cheap and easy-to-build weapon usually could be relied upon to work. In the 1950s Allied forces, as well as British commandos, used the British-made Sten MKIIS in the Korean War. In the Vietnam era, the U.S. created a military version of a Ruger 10–22 semi-automatic Carbine that saw heavy use. In more recent years, military snipers have used a great variety of rifle makes in combat, though the AK-47 remains especially popular.

The development of a supremely effective silencer has been complicated by many factors. The noise made by the discharge of a firearm has three components: 1) the sounds made by the movement of the parts of the gun; 2) the crack of a bullet passing through the atmosphere at a rate above the speed of sound; and 3) the release of high pressure gases breaking out of the barrel. Silencers only address the last concern, although the use of a heavy subsonic bullet rather than a high velocity bullet greatly adds to sound suppression. High velocity bullets make a noise of their own when traveling through the air outside of the silencer, and the substitution of a slower bullet will slow the passage of the projectile through the air, thereby reducing ballistic noise. Silencers that fire regular supersonic ammunition are only a little quieter than those without suppressors. Subsonic ammunition has less power than regular ammunition, making it effective only at shorter ranges of up to 600 feet (200 meters). Silencers can be attached to most firearms, but they work best as components of purpose built or modified guns.

Silencers are now made for almost every firearm, from fully automatic submachine guns to big bore bolt-action rifles, and the popularity of these weapons is likely to grow. Silencers make it easier to identify the enemy, easier to shoot the enemy, and harder to be detected by the enemy. Particularly suited for guerrilla warfare as well as secret operations and law enforcement, sound suppressors have become standard issue equipment for intelligence agents and security forces.

FURTHER READING:

BOOKS:

Truby, J. David. *Silencers, Snipers and Assassins: An Overview of Whispering Death.* Boulder, CO: Paladin Press, 1972.

White, Mark. *On the Control of Silencers, Interpol: The International Criminal Police Organization.* Washington, D.C.: Government Printing Office, 2002.

SEE ALSO

Assassination Weapons, Mechanical
CIA (United States Central Intelligence Agency)
Espionage
Intelligence Agent
OSS (United States Office of Strategic Services
U-2 Incident

Skunk Works

"Skunk Works" is the nickname for the headquarters of advanced development programs for Lockheed Martin Aeronautics Company at Palmdale, California, some 80 miles (128 km) north of Los Angeles in the Antelope Valley. Established in 1943 by what was then known as the Lockheed Aircraft Corporation, the Skunk Works has been the birthplace of numerous extraordinary aircraft, including the U-2 and SR-71 reconnaissance planes and the F-117A stealth fighter.

During World War II, Lockheed established the facility, under the direction of Clarence L. (Kelly) Johnson, to build the ultra-secret P-80 Shooting Star, the first jet-propelled fighter in the U.S. air fleet. The Skunk Works got its name from a nearby chemical plant, the noxious odors of which wafted toward the Lockheed facility on windy days. Technicians there referred to the plant as the "skunk works," a term taken from the comic strip *L'il Abner* by Al Capp, and eventually the nickname became attached to the facility itself.

Over the decades that followed, the Skunk Works produced the U-2 in the 1950s, the A-12 Oxcart and SR-71 Blackbird in the 1960s, and the F-117A Nighthawk in the 1980s. It also adapted the C-130, used for troop transport by airborne forces, for special missions. The Skunk Works even built a ship, the U.S. Navy research vessel *Sea Shadow.*

In addition, engineers at the Skunk Works developed the CL-282 and CL-400, two craft that were never went into use. The first of these, introduced in 1958, was to be a high-altitude reconnaissance craft, but plans for it were

NASA selected the Lockheed-Martin Skunk Works to build and test the technology demonstrator VentureStar, as shown in this computer-generated concept. Skunk Works emerged from the cloak of secrecy that has shrouded it since the Cold War. AP/WIDE WORLD PHOTOS.

scrapped in favor of the U-2. The CL-400 was to be a successor to the U-2, based on Johnson's design for a hydrogen-powered supersonic craft. However, the results satisfied neither Lockheed nor the Air Force, and the project was abandoned in October 1957.

FURTHER READING:

BOOKS:

Bennis, Warren G., and Patricia Ward Biederman. *Organizing Genius: The Secrets of Creative Collaboration.* Reading, MA: Addison-Wesley, 1997.

Jenkins, Dennis R. *Lockheed Secret Projects: Inside the Skunk Works.* St. Paul, MN: MBI Publishing, 2001.

Miller, Jay. *Lockheed Martin's Skunk Works.* North Branch, MN: Specialty Press, 1995.

Pace, Steve. *Lockheed Skunk Works.* Osceola, WI: Motorbooks International, 1992.

Rich, Ben R., and Leo Janos. *Skunk Works: A Personal Memoir of My Years at Lockheed.* Boston: Little, Brown, 1994.

ELECTRONIC:

Lockheed Martin Aeronautics Company. <http://www.lmaeronautics.com/palmdale/> (April 2, 2003).

SEE ALSO

F-117A Stealth Fighter
Photography, High-Altitude
SR-71 Blackbird
U-2 Spy Plane
Vietnam War

Slovakia, Intelligence and Security

The security and intelligence agencies of Slovakia work in the shadow cast by their communist-era predecessors. In

a situation common among many nations of the former Soviet bloc, Western observers have noted a distressing degree of continuity between the old police-state security and intelligence apparatus, and that of the new democratic state. At the same time, Slovakia has worked to fulfill the requirements of integration into the new, post-communist Europe.

In 1993, Slovakia separated from the Czech Republic, with which it had comprised the nation of Czechoslovakia. Citizens of that nation had, during the years of communist rule, come to fear the State Security Service, or StBU. By 1993, the StBU had been disbanded, but four years later, Radio Free Europe reported that much of the infrastructure of the StBU lingered on under the guise of the new Slovenska Informacna Sluzba (Slovak Information Service, or SIS). According to the American information service, the Slovak government regularly conducted surveillance operations on its citizenry through the SIS.

A decade later, Slovakia was under consideration for membership in both the European Union (EU) and the North Atlantic Treaty Organization (NATO), both of which require democratization as a prerequisite for admission. At the same time Slovakia had progressed toward greater democracy, its security and intelligence services had improved their ability to protect sensitive secrets. Among the requirements NATO imposed was the establishment of the National Security Office (NBU), which officially began operating in November 2001. The purpose of NBU is, in part, to protect classified information, which is shared between member nations.

In December 2002, members of the European Union approved Slovakia for membership in the EU beginning in 2004.

FURTHER READING:

BOOKS:

Williams, Kieran, and Dennis Deletant. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania.* New York: Palgrave, 2001.

PERIODICALS:

Gill, Peter. Review of *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania. Slavic Review* 61, no. 2 (2002): 375–76.

ELECTRONIC:

Naegele, Jolyon. Slovakia: Intelligence Service Reverts to Communist-Era Practices. Radio Free Europe/Radio Liberty. <http://www.rferl.org/nca/features/1997/05/F.RU.97052913316.html> (March 1, 2003).

Slovakia: Intelligence. Federation of American Scientists. <http://www.fas.org/irp/world/slovakia/index.html> (March 1, 2003).

SEE ALSO

Czech Republic, Intelligence and Security
Hungary, Intelligence and Security
Poland, Intelligence and Security

Slovenia, Intelligence and Security

The principal intelligence agency in Slovenia is the *Slovenska Obvesèevalno-Varnostna Agencija* (SOVA; Slovenian Intelligence and Security Agency). Domestic security priorities set by the national assembly guide SOVA, which is responsible for collecting information both at home and abroad on groups or individuals who might threaten the state and its constitutional system.

Other components of the Slovenian intelligence and security apparatus include the national defense ministry, under whose aegis are the 1st Special Brigade of the Slovenian Army, also known as the Ministry of Defense Reconnaissance and Intervention Service (MORIS), as well as the Ministry of Defense Intelligence and Security Service (VOMO). Additionally, the Ministry of the Interior, Ministry of Foreign Affairs, National Police Force, and Customs Service all have security and/or intelligence roles.

Slovenia's security depends to a large extent on the integration of policies and resources involving the United Nations, the Organization for Security and Cooperation in Europe, the European Union (EU), and NATO—especially with regard to establishing long-term stability in the Balkans.

In December 2002, members of the European Union approved Slovenia for membership in the EU beginning in 2004.

FURTHER READING:

ELECTRONIC:

Slovene Intelligence and Security Agency. <http://www.sigov.si/vrs/ang/ang-text/ministries/slovene-intelligence-and-security-agency.html> (March 1, 2003).

Slovenia: Intelligence. Federation of American Scientists. <http://www.fas.org/irp/world/slovenia/index.html> (March 1, 2003).

SEE ALSO

Bosnia, Intelligence and Security
Croatia, Intelligence and Security
Serbia, Intelligence and Security

Smallpox

Smallpox is an infection caused by the variola virus, a member of the poxvirus family. The disease is highly

infectious. Passage from person to person via contaminated aerosolized droplets (from sneezing, for example) occurs easily, and so the spread of smallpox through a population can occur quickly. Like most viruses and other microorganisms, the variola virus can be transported from one location to another without difficulty, thus making smallpox a potentially attractive choice for biological warfare and a serious threat as a weapon of bioterrorists.

Smallpox is a highly contagious disease. The virus can spread by direct contact with those who are infected, in contaminated air droplets, and even by touching objects such as books and blankets that have been previously used by someone who has smallpox.

When infected with the virus, there is a 12–14 day symptom-free period, during which the virus is multiplying in the body. There is then a sudden onset of symptoms. The symptoms include fever and chills, muscle aches, and a flat, reddish-purple rash on the chest, abdomen, and back. These symptoms last about three days, after which the rash fades and the fever drops. A day or two later, the fever returns, along with a bumpy rash starting on the feet, hands, and face. This rash progresses from the feet along the legs, from the hands along the arms, and from the face down the neck, ultimately reaching and including the chest, abdomen, and back. The individual bumps, or papules, fill with clear fluid, and, over the course of 10–12 days, became pus-filled. The pox eventually scabs over, and when the scab falls off it leaves behind a pock-mark or pit, which remains as a permanent scar on the skin of the victim.

Smallpox can be lethal, usually due to bacterial infection of the open skin lesions, pneumonia, or bone infections. A severe and quickly fatal form of smallpox is known as "sledgehammer smallpox." This form of smallpox is characterized by bleeding from the skin lesions, as well as from the mouth, nose, and other areas of the body.

Smallpox has been present for thousands of years. For example, studies of the mummy of Pharaoh Ramses V, who died in 1157 B.C., revealed symptoms of smallpox infection.

Large smallpox epidemics have occurred throughout recorded history. Attempts to protect against smallpox infection began centuries ago, even thought the microbiological nature of the disease was then unknown. In the tenth century, accounts from China, India, and the Americas describe how individuals who had even a mild case of smallpox could not be infected again. Fluid or pus from the skin lesions was scratched into the skin of those who had never had the illness, in an attempt to produce a mild reaction and its accompanying protective effect. Unfortunately, these efforts sometimes resulted in full-fledged smallpox, and helped spread the infection. Such crude vaccinations against smallpox were outlawed in Colonial America.

In 1798, Edward Jenner published his observation that milkmaids who contracted cowpox infection caused by vaccinia virus (a relative of variola) were immune to smallpox. He used infected material from the cowpox lesions to prepare an injection that helped protect the humans. Although Jenner's development of immunization was harshly criticized at first, the work paved the way for the development of vaccines.

Until the development of a smallpox vaccine, no treatment for smallpox was known, nor could anything shorten the course of the disease. Until its eradication, smallpox was diagnosed most clearly from the patients' symptoms. Electron microscopic studies could identify the variola virus in fluid isolated from disease papules, from infected urine, or from the blood prior to the appearance of the papular rash.

In the 1960s, the World Health organization (WHO) began a campaign to treat people infected with smallpox and vaccinate those who might be exposed to the infection. The WHO program was extremely successful, and the virus was declared eradicated worldwide in May of 1980. Stored stocks of the virus were maintained in two laboratories. One is housed at the Centers for Disease Control and Prevention in Atlanta, Georgia. The other smallpox stock is maintained in Russia.

These stocks were slated to be destroyed in the late 1990s however, U.S. President William J. Clinton halted plans for destruction of the American stocks. Concern that another poxvirus could mutate (undergo genetic changes) and cause human infection, along with the possible use of smallpox as a bioterrorist weapon or as a weapon of state-sanctioned war, has made preservation of the smallpox stock for vaccine development purposes important. As of early 2003, the stocks remain undisturbed.

FURTHER READING:

BOOKS:

Hopkins, D. R. *The Greatest Killer: Smallpox in History.* Chicago: University of Chicago Press, 2002.

Preston, R. *The Demon in the Freezer.* New York: Random House, 2002.

PERIODICALS:

Henderson, D. A., T. V. Inglesby, J. G. Bartlett, et al. "Smallpox as a Biological Weapon: Medical and Public Health Management." *Journal of the American Medical Association* no. 281 (1999): 2127–137.

ELECTRONIC:

Centers for Diseases Control and Prevention. "Smallpox." Public Health Emergency Preparedness and Response. November 26, 2002. <http://www.bt.cdc.gov/agent/smallpox/index.asp>(27 November 2002).

SEE ALSO

Biocontainment Laboratories

Biological Weapons, Genetic Identification Bioterrorism

Smallpox Vaccine

BRIAN HOYLE

Smallpox, or variola major, is a highly contagious disease that is caused by the variola virus. The name smallpox comes from the Latin word for spotted. A visual hallmark of smallpox is the raised bumps that appear on the victim's face and body. Smallpox is fatal in approximately 25% of cases.

There is no cure for smallpox, and treatment is supportive. Prevention of the disease by the administration of smallpox vaccine is the most effective strategy to eliminate the spread of smallpox. Vaccination, conducted on a worldwide scale, was successful in effectively eliminating smallpox as a naturally occurring disease.

The eradication of smallpox saw the end of routine vaccination programs. As of 2003, no American under the age of 30 routinely receives the vaccine. Even in older Americans, immunity has likely faded. After the bioterrorist anthrax attacks on U.S. citizens in late 2001, concern has heightened that smallpox will be used as a terrorist weapon on a population that is once again susceptible to infection. Beginning in January, 2003, health care workers at strategic hospitals and research centers across the United States received the smallpox vaccine in order to provide a population of immune responders in case of a smallpox outbreak or mass exposure due to bioterrorism. Mass vaccination programs are again under study by researchers, and smallpox vaccines are scheduled to be available to all Americans on a voluntary basis by mid-2004.

The only smallpox vaccine that is in use today—a preparation called Dryvax—is made from vaccinia, a poxvirus that is very similar to the smallpox virus. The reaction of the immune system to vaccinia confers protection to the smallpox virus. The vaccinia virus that is administered is alive and causes a mild infection, which is inconsequential in most people. However, in a small minority of people, the use of the live virus does carry a risk that the virus will spread from the site of injection, and that side effects will result.

The side effects are typically minor (e.g., sore arm at the injection site, a fever, and generalized body aches). However, rare severe side effects are possible, which can even be life threatening. These include encephalitis (a swelling of the brain and spinal cord), gangrene, extreme eczema, and blindness. People whose immune systems are not functioning properly are especially at risk, as are those people who have had skin ailments such as eczema or atopic dermatitis. The fatality rate due to the vaccine is estimated to be one in eight million.

Despite the risk, smallpox vaccine is worthwhile if exposure to smallpox is possible. A single injection of vaccinia vaccine preparation provides up to five years of immunity to smallpox. A subsequent injection extends this protection. Studies have demonstrated that up to 95% of vaccinated people are protected from smallpox infection. Protection results after just a few days. If exposure to smallpox is anticipated—such as in a military campaign—vaccination a short time before can be a wise precaution.

Smallpox vaccine is injected using a two-pronged needle dipped into the vaccine solution, which then pricks the skin of an upper arm several times in a few seconds. The injection typically becomes sore, blisters and forms a scab. When the scab falls off, a distinctive scar is left.

Currently, the stockpile of smallpox vaccine in the U.S. is about 15 million doses. The vaccine may be capable of being diluted 10 times without losing its protective potency. This would extend the coverage to 150 million people. As of December 2002, 155 million additional doses of smallpox vaccine are being delivered. The new vaccine is made from cow tissues that were grown in laboratory culture. This technique produces a more uniform vaccine preparation than the old method, where tissue was scraped from the lesions of infected cows.

Other smallpox vaccines. The development of improved smallpox vaccines, and the refinement of existing vaccine preparations, has begun only recently. Research on improved vaccines largely ended when the demand for vaccinations ended in the 1970s.

A form of smallpox vaccine called Modified vaccinia Ankara (MVA) was developed 40 years ago. The vaccinia virus used in this preparation cannot replicate in human cells, but still generates an immune response. While the vaccine appears to produce fewer side effects than the standard vaccinia vaccine, large scale tests have not yet been done.

Another vaccinia strain that has been used to develop a smallpox vaccine is called LC16m8. In contrast to MVA, LC16m8 does replicate inside human cells. However, the virus lacks some of the usual surface proteins that may be important in the immune response.

Genetic engineering is also playing a role in smallpox vaccine development. For example, a vaccinia strain has been engineered that does not form certain proteins unless the antibiotic tetracycline is present. The idea here is that the vaccine and the antibiotic would be taken simultaneously. In the event of an adverse vaccine reaction, use of the antibiotic would be stopped, which would stop the immune reactivity of the vaccinia virus. This approach is still in the laboratory stage.

A Canton, Massachusetts, police officer, left, is seen outside the offices of Acambis Inc., a licensed producer of smallpox vaccine, in October 2001. The fear of bioterrorism attacks has spurred federal officials to ask the British-owned company to speed up production of the vaccine. AP/WIDE WORLD PHOTOS.

FURTHER READING:

BOOKS:

Institute of Medicine. *Assessment of Future Scientific Needs for Live Variola Virus.* Washington, DC: National Academy Press, 1999.

PERIODICALS:

Henderson, D.A. "Smallpox: clinical and epidemiologic features." *Emerging Infectious Diseases* no. 5 (1999): 537–39.

Rosenthal, S.R., M. Merchlinsky, C. Kleppinger, et al. "Developing New Smallpox Vaccines." *Emerging Infectious Diseases* no. 7 (2001): 920–26.

ELECTRONIC:

Centers for Disease Control and Prevention. "Smallpox Factsheet: Vaccine Overview." Public Health Emergency Preparedness and Response. December 9, 2002. <http://www.bt.cdc.gov/agent/smallpox/vaccination/facts.asp>(31 December 2002).

SEE ALSO

Biological Warfare
Infectious disease, threats to security
NNSA (United States National Nuclear Security Administration)
Weapons of Mass Destruction, Detection

SOE (Special Operations Executive)

CARYN E. NEUMANN

A World War II-era British secret service division, the Special Operations Executive (SOE), formed on July 19, 1940, to coordinate subversion and sabotage in enemy-occupied countries. SOE agents distributed propaganda, blew up bridges, directed air strikes, destroyed factories, and taught resistance tactics. Most of SOE's success came in France, Yugoslavia, Greece, and Italy, although it also conducted major operations in Albania, Abyssinia, Belgium, Burma, China, Denmark, Hungary, Malaya, Norway, Poland, Romania, Siam (present-day Thailand), Turkey, and the Dutch East Indies. SOE disbanded on January 15, 1946, with many of its agents moving to MI6.

With the fall of France in 1940, SOE received authorization to begin operations to divert German, Italian, and Japanese attention away from the main fighting fronts towards the rear areas. The division, with headquarters scattered throughout London, developed three branches: SO1 for propaganda, SO2 for active operations, and SO3 for planning. Resistance movements had already formed

in occupied countries, and it fell to SOE to finance, supply, and direct these operations. It did not operate effectively in the main enemy homelands of Germany and Japan because the locals were too unfriendly and the police too strong.

In order to achieve its goals, SOE relied upon 470 agents, 117 of whom died in action. The agents generally parachuted behind the lines to teach unarmed combat, bomb building, and espionage strategies to resistance fighters, but a number were pulled from the criminal ranks to supply expertly forged documents. SOE's greatest success may have been the 1942 bombing of a Norwegian plant that supplied heavy water (deuterium oxide) to Germany for use in developing an atomic bomb. Another notable achievement came when SOE agents guided a Royal Air Force attack on Gestapo headquarters in Denmark that permitted one prisoner escaping from the rubble to pick up a file of the names of Danish collaborators to be used as evidence at treason trials after the war. SOE so succeeded in harassing the Axis powers that they pulled troops from the front lines and sent them to guard railways, storage depots, and factories, while the British in contrast simply relied upon old men to protect these facilities.

An accurate measure of SOE's impact is difficult. The requirements of clandestine work meant that SOE agents rarely left written records, and those few official papers that do exist have been classified secret by the British government. The little that is known about the division marks it as a success.

■ FURTHER READING:

BOOKS:

Foot, M.R.D. *SOE: An Outline History of the Special Operations Executive 1940–46.* London: British Broadcasting Corporation, 1984.

SEE ALSO

Covert operations
Espionage
French Underground During World War II, Communication and Codes
Gestapo
MI6 (British Secret Intelligence Service)
Nuclear Weapons
Propaganda, Uses and Psychology
Sabotage

Soldier and Biological Chemical Command (SBCCOM), United States Army

The United States Army Soldier and Biological Chemical Command (SBCCOM) is a support organization focused on the development, response to, and safe handling of chemical weapons. Formed in 1998 from the merger of two earlier groups, SBCCOM is heavily involved in preparedness training for both military and civilians to prevent or, if necessary, respond to terrorist attacks.

In December 1998, the United States Army combined its Chemical and Biological Defense Command and its Soldier Systems Command to form SBCCOM. The new command, which brought together expertise in soldier, chemical, and biological areas, was responsible for research, development, and implementation of chemical, biological, and soldier missions. It would also oversee the chemical weapons stockpile of the United States Army from its headquarters in the Edgewood Area of the Aberdeen Proving Ground in Maryland.

Mission. The mission of SBCCOM is to develop, integrate, acquire, and sustain soldier and NBC [nuclear, biological, and chemical] defense technology, systems, and services to ensure the decisive edge and maximum protection for the United States. Provide for the safe storage, treaty compliance, and destruction of classified material.

To this end, the command is involved in three principal areas: research, development, and acquisition of chemical and biological weapons and defense systems; emergency preparedness and response in the event of attack; and the safe, secure storage, remediation, and demilitarization of chemical and biological weapons.

Realizing mission objectives. Research takes place in two principal centers. At the Edgewood Chemical Biological Center, project managers undertake concept exploration, demonstration, validation, and emergency manufacturing development for production of chemical defense systems, aerosol systems, flame weapons, and obscuring smoke. At the Soldier Systems Center in Natick, Massachusetts, SBCCOM analysts address problems of total lifecycle management for the soldier through centralized development, procurement, and integration. These issues involve matters such as shelters, airdrops, field service, and organizational equipment.

SBCCOM oversees the safe and secure storage of chemical weapons at eight depots scattered across the United States: Edgewood, Maryland; Blue Grass, Kentucky; Newport, Indiana; Anniston, Alabama; Pine Bluff, Arkansas; Pueblo, Colorado; Tooele, Utah; and Umatilla, Oregon. At these sites, SBCCOM also regulates U.S. compliance with international treaties on chemical weapons. Additionally, a post at Rocky Mountain Arsenal in Colorado is charged with safely destroying old chemical weapons.

In the area of emergency preparedness and response, SBCCOM directs the Army Technical Escort Unit, which is globally deployable and has a history that goes back to the Korean War. (Other aspects of SBCCOM activities date to the period between the world wars, which saw early

efforts to control the spread and use of the chemical weapons that had been displayed with such gruesome effect on the Western Front in World War I.) SBCCOM also leads the Domestic Preparedness Program, which in 1998 made the news with education efforts in 120 cities nationwide.

FURTHER READING:

PERIODICALS:

Dezelan, Louis A. "Preparing for Terrorism." *Law & Order* 46, no. 10 (October 1998): 107–110.

Thompson, Neal. "Preparing for Disaster." *The Sun.* (Baltimore, MD) (March 13, 1998): 3B.

ELECTRONIC:

United States Army Soldier and Biological Chemical Command (SBCCOM). <http://www.sbccom.army.mil/> (January 27, 2003).

SEE ALSO

Chemical Safety: Emergency Responses

Solid-Phase Microextraction Techniques

Solid-phase microextraction (SPME) is a chemical technique designed to detect chemical compounds. In its forensic application, it is used to find chemical warfare agents, high explosives, or illegal drugs. Among the world's leading research institutes in forensic SPME work is Lawrence Livermore National Laboratory's Forensic Science Center (FSC) in San Francisco. Established in 1991, the FSC, which had 15 staff members in 2002, implements a variety of research tools in forensics. Among these is SPME, which makes use of optical fibers to collect chemical samples.

Extremely small, these fibers are about 100 micrometers thick—the width of a human hair. Stored in syringes, they are coated with chemicals made to respond to specific substances such as particular explosives or drugs. With a minimum of disruption and effort, these "chemical dipsticks" can collect thousands of compounds.

One of the few drawbacks of the fibers used in SPME is the fact that they are extremely fragile, and for this reason, the FSC developed durable aluminum storage tubes. They have also provided the Federal Bureau of Investigation with portable SPME field kits, as well as a transport tube small enough to fit in a shirt pocket. The FSC is licensing both versions to private industry for sale to the federal government.

SPME has been used at the FSC to monitor the safety of nuclear warheads as part of the Stockpile Stewardship Program. After collecting samples of volatile and semivolatile molecules formed from the breakdown of organic polymers and high explosives, scientists look for signs that corroded parts may need to be replaced.

FURTHER READING:

PERIODICALS:

Bodrain, Rosemarie R. "Analysis of Exempt Paint Solvents by Gas Chromatography Using Solid-Phase Microextraction." *JCT, Journal of Coatings Technology* 72, no. 900 (January 2000): 69–74.

Comello, Vic. "Researchers Are Giving SPME a Second Look." *Research & Development* 41, no. 2 (February 1999): 44–45.

Marsili, Ray. "New Techniques Revolutionize Analyses of Liquid Samples." *Research & Development* 42, no. 2 (February 2000): 22–24.

ELECTRONIC:

Counterterrorism and Incident Response. Lawrence Livermore National Laboratory. <http://www.llnl.gov/nai/rdiv/rdiv.html> (April 2, 2003).

Solid-Phase Microextraction (SPME). Science & Technology, Lawrence Livermore National Laboratory. <http://www-cms.llnl.gov/s-t/solid_phase.html> (April 2, 2003).

SEE ALSO

Chemistry: Applications in Espionage, Intelligence, and Security Issues
Forensic Science
Gas Chromatograph-Mass Spectrometer
Lawrence Livermore National Laboratory (LLNL)

Soman

BRIAN HOYLE

Soman (or "GD") is a synthetic (human-made) compound that affects the functioning of nerves. As such, Soman is one of a group of chemicals that are known as nerve agents.

Soman was developed in Germany in 1944. Its original purpose was as an insecticide. The chemical, which does not occur naturally in the environment, is similar to the group of insect poisons (pesticides) called organophosphates, both in activity and in how they are applied (i.e., airborne release). However, Soman (and nerve agents in general) are much more potent and deadly than the insect nerve poisons.

Several properties of Soman are responsible for its potency. It is normally a clear, colorless, and tasteless liquid, and so is not easily detected. While it typically has a slight odor reminiscent of rotting fruit, this smell can be disguised upon mixing with water or food. Even wetting

the skin with soman-contaminated water can be lethal, as the poison is absorbed through the skin. In addition, Soman can vaporize when heated, and retains its toxicity when inhaled. The vapor can even cling to clothing and affect others as is it released from the clothing.

The effects of Soman begin almost immediately upon exposure. Within minutes to hours the nerves that control the functioning of muscles are inhibited from turning off the stimuli that trigger muscle activity. At the molecular level, this occurs via the inactivation of an enzyme that breaks apart another chemical that acts as a bridge between adjacent nerve cells, and so allows a nerve impulse to flow. Because the bridging chemical remains intact, nerve impulses cannot be controlled or turned off. As a result of the constant activity, muscles such as the lungs tire and can cease to function. Some of the symptoms associated with Soman exposure include watery and painful eyes, coughing, rapid breathing, diarrhea, confusion, headache, slow or fast heart rate, and, in severe cases, unconsciousness, convulsions, and respiratory failure.

These effects occur for only a short time after Soman vapor is released into the atmosphere, since it is a very volatile compound. When incorporated into water or food, however, Soman can remain active and deadly for a longer time.

The damage due to Soman is cumulative. Because the chemical can persist in the body, repeated exposure increases the concentration of Soman in the body. People in low-lying areas and valleys can be especially susceptible, as Soman is more dense than air and so "settles out" near the bottom of depressions.

Soman was one of the nerve agents that may have been used against the people of Iran by the government of Iraq under Suddam Hussein during the Iran-Iraq war in the 1980s. Soman once also once produced as a chemical weapon by the United States. Production by the United States ceased decades ago.

FURTHER READING:

BOOKS:

Government of the United States. *21st Century Complete Guide to Chemical Weapons and Chemical Terrorism—U.S. Demilitarization Program, Stockpile Destruction Emergency Plans, Nerve Gas and Blister Agent Civilian Treatement and First Aid, Home Sheltering Plans.* Washington, DC: Progressive Management, 2002.

ELECTRONIC:

Agency for Toxic Substances and Disease Registry. "Nerve Agents (GA, GB, GD, VX)." Division of Toxicology, Centers for Disease Control and Prevention. March 13, 2003. <http://www.atsdr.cdc.gov/tfactsd4.html>(April 10, 2003).

Agency for Toxic Substances and Disease Registry. "Facts about Soman." Division of Toxicology, Centers for Disease Control and Prevention. March 12, 2003. <http://www.bt.cdc.gov/agent/soman/basics/facts.asp>(April 10, 2003).

SEE ALSO

Chemical Warfare
Mustard Gas
Sarin Gas

SONAR

K. LEE LERNER

SONAR, an acronym for Sound Navigation and Ranging, is a technique based on echolocation used for the detection of objects underwater.

Historical development of SONAR. Ancient drawings depict the use of long tubes as non-mechanical underwater listening devices to detect and transmit sound in water. In the late nineteenth century, scientists began to explore the physical properties associated with sound transmission in water. In 1882, a Swiss physicist, Daviel Colladen, attempted to calculate the speed of sound in the known depths of Lake Geneva. Based upon the physics of sound transmission articulated by English physicist Lord Rayleigh (1842–1914), and the piezoelectric effect discovered by French scientist Pierre Curie (1509–1906), in 1915, French physicist Paul Langevin (1872–1946) invented the first system designed to utilize sound waves and acoustical echoes in an underwater detection device.

In the wake of the *Titanic* disaster, Langevin and his colleague Constantin Chilowsky, a Russian engineer then living in Switzerland, developed what they termed a "hydrophone" as a mechanism for ships to more readily detect icebergs (the vast majority of any iceberg remains below the ocean surface). Similar systems were put to immediate use as an aid to underwater navigation by submarines.

Improved electronics and technology allowed the production of greatly improved listening and recording devices. Because passive SONAR is essentially nothing more than an elaborate recording and sound amplification device, these systems suffered because they were dependent upon the strength of the sound signal coming from the target. The signals or waves received could be typed (i.e. related to specific targets) for identifying characteristics. Although skilled and experienced operators could provide reasonably accurate estimates of range, bearing, and relative motion of targets, these estimates were far less precise and accurate than results obtained from active systems unless the targets were very close—or were very noisy.

The threat of submarine warfare during World War I made urgent the development of SONAR and other means of echo detection. The development of the acoustic transducer that converted electrical energy to sound waves

enabled the rapid advances in SONAR design and technology during the last years of the war. Although active SONAR was developed too late to be widely used during World War I the push for its development produced enormous technological dividends. Early into World War II, the British Anti-Submarine Detection and Investigation Committee (its acronym, ASDIC, became a name commonly applied to British SONAR systems) made efforts to outfit every ship in the British fleet with advanced detection devices. The use of ASDIC proved pivotal in the British effort to repel damaging attacks by German submarines.

SONAR and RADAR. Although they rely on two fundamentally different types of wave transmission, SONAR and Radio Detection And Ranging (RADAR) and both are remote sensing systems. While active SONAR transmits acoustic (i.e., sound) waves, RADAR sends out and measures the return of electromagnetic waves.

In both systems these waves return echoes from certain features or targets that allow the determination of important properties or attributes of the target (e.g., shape, size, speed, distance to target, etc.). Because electromagnetic waves are strongly attenuated (diminished) in water, RADAR signals are mostly used for ground or atmospheric observations. Because SONAR signals easily penetrate water, they are ideal for navigation and measurement under water. Within the ocean, the speed of sound varies with changes in temperature and pressure, and these conditions can also be determined by alterations in SONAR signals.

SONAR usually operates at frequencies in the 10,000–50,000 Hz range. Higher higher frequencies provide more accurate location data, but propagation losses (i.e. loss of signal strength over distance) also increase with frequency.

■ FURTHER READING:

BOOKS:

Van Trees, Harry L. *Radar-Sonar Signal Processing and Gaussian Signals in Noise.* Indianapolis, IN: John Wiley & Sons, 2001.

Waite, A. D. *Sonar for Practising Engineers.* Indianapolis, IN: John Wiley & Sons, 2001.

ELECTRONIC:

Canadian Center for Remote Sensing, "History of Remote Sensing." 2001. <http://www.ccrs.nrcan.gc.ca/ccrs/org/history/morleye.htm> (February 1, 2003).

SEE ALSO

P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft
Remote Sensing
SOSUS (Sound Surveillance System)
Undersea Espionage: Nuclear vs. Fast Attack Subs

SOSUS (Sound Surveillance System)

■ K. LEE LERNER

Utilizing the unique properties of sound transmission in water, during the 1950s, the United States Navy developed the Sound Surveillance System (SOSUS). Code named "Jezebel" the SOSUS system provided critical monitoring of Soviet submarine and ship movements, especially through the critical ocean gaps between Greenland, Iceland, and the United Kingdom (the GI-UK gap). SOSUS systems were so sensitive that trained observers could determine ship type—and in some cases, identify specific ships.

SOSUS used arrays of hydrophones (underwater microphones) strategically placed along the ocean bottom. The hydrophones were connected by cables to onshore monitoring stations.

In addition to localized sound readings (i.e., sounds detected within the expected range of the hydrophones), SOSUS also picked up sounds channeled through specific conditions of state (i.e., pressure, temperature) or salinity that create channels though which sound waves propagate over long distances with minimal resistance and minimal loss of strength. This sound fixing and ranging channel (SOFAR channel) was discovered independently by American and Soviet scientists in 1943 during World War II.

SOFAR channels are capable of transmitting the low frequency, long wavelength sound waves produced by an explosion. Sound waves can be trapped effectively in SOFAR channels and propagate with little loss of energy over distances in excess of 15,500 miles (25,0000 km).

Naval communication systems utilize low frequency, long wavelength signals to enhance communications with submerged submarines. Prior to the widespread use of Global Positioning System (GPS) equipment, the SOFAR channel was also used for navigation and the location of marine craft. Evidence gathered by marine biologists indicates that certain species of whales utilize the SOFAR channel to communicate mating calls over long distances.

In general, the speed of sound depends upon the medium through which the sound waves propagate and the properties of the medium (e.g., state, temperature, pressure, salinity, etc.) Accordingly, the speed of sound differs in air, fresh water, and oceanic saltwater.

Within the ocean, the speed of sound varies with changes in temperature and pressure. When the near-surface layer is well mixed by currents and surface action, the resulting isothermal layer provides uniform propagation of sound. When a temperature gradient exists (e.g., a temperature decrease with increasing depth), the resulting thermocline shows a characteristic decrease in the

speed of sound with decreasing temperature. At some depth (approximately 420 fathoms or 750 meters), the variations in temperature become so slight that the water becomes isothermal. As depth increases, so does the pressure. Because pressure is directly proportional to sound wave transmission speeds, as the pressure increases with depth so does the speed of sound.

Specific combinations of temperature, pressure, and salinity may act to create "shadow zones" that are resistant to the propagation of sound waves or that act as reflectors of sound waves. Soviet submarine captains attempted to use these zone or layer to conceal their ships from detection by surface SONAR arrays. The layers could also to "bend" signals detected by the SOSUS array in order to attempt to conceal ship movements. In practice, staying within such layers proved impossible to maintain for extended periods, and intermittent SOSUS plots could be used to track ship movements or provide a probable position to explore with the use of sonar buoys dropped by airplane.

Surface sonar buoys were also used to fill gaps in the SOSUS listening network.

FURTHER READING:

BOOKS:

Munk W., Worcester P., and C. Wunsch. *Ocean Acoustic Tomography.* Cambridge: Cambridge University Press, 1995.

SEE ALSO

P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft
Undersea Espionage: Nuclear vs. Fast Attack Subs

South Africa, Intelligence and Security

After decades of segregation under the system of apartheid, South Africa in 1994 became a multiracial democracy. In place of the old regime, which included the dreaded Bureau of State Security—BOSS, a agency portrayed memorably by British author Graham Greene in *The Human Factor* (1978)—the new South Africa had its own intelligence and security organizations. Included among these are the National Defense Force Intelligence Division, the National Intelligence Agency (NIA), the South African Police Service (SAPS), the South African Secret Service (SASS), and the National Intelligence Coordinating Committee (NICOC), which oversees these agencies.

The South African National Defense Force (SANDF) consists of four military organizations—army, navy, air force, and medical service—as well as support services. It was formed from the integration of the old South African Defense Force with the armies of the three former racial homelands (Transkei, Bophuthatswana, and Venda), as well as those of political parties, including the African National Congress (ANC), Pan Africanist Congress (PAC), Umkhonto weSiswe, and the Azanian People's Liberation Army. Similarly, NIA was formed from a combination of the old National Intelligence Service with the intelligence services of ANC, PAC, and the three former homeland intelligence services, and the ANC and PAC. Likewise SAPS is an amalgam of the old South African Police and 10 former homeland agencies.

The SANDF Intelligence Division collects and evaluates military intelligence, and supplies this as needed to national leadership. NIA is charged with collecting domestic intelligence concerning persons or groups who may potentially threaten the security of the republic or its people. Among the special units of SAPS are the Crime Combatting and Investigation Division; the National Investigative Service, whose roles include counterintelligence work with NIA; the Visible Policing Division, a crime-prevention organization; and the Special Guard Unit, which performs a bodyguard function similar to that of the U.S. Secret Service. SASS conducts foreign intelligence and counterintelligence operations.

NICOC, which reports to the president and cabinet, brings together the Coordinator for Intelligence, the Director-General of NIA, the chief of the National Defense Force Intelligence Division, the head of the National Investigation Service of SAPS, and the Director-General of SASS. It thus serves as a "joint chiefs of staff" for the South African intelligence community.

FURTHER READING:

BOOKS:

McCarthy, Shaun. *Intelligence Services for a Democratic South Africa: Ensuring Parliamentary Control.* London: Research for the Study of Conflict and Terrorism, 1996.

Winter, Gordon. *Inside BOSS: South Africa's Secret Police.* London: Allen Lane, 1981.

PERIODICALS:

Mallet, Victor. "Pretoria Faces German Bugging Protest." *Financial Times* (November 22, 1999): 10.

"Thabo's Watching: Spying in South Africa." *The Economist* 362, no. 8266 (March 30, 2002): 41.

ELECTRONIC:

South African Department of Defence. <http://www.mil.za/> (March 1, 2003).

South African Intelligence Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/rsa/index.html> (March 1, 2003).

South Korea, Intelligence and Security

South Korea, or the Republic of Korea (ROK), has an intelligence and security apparatus that is, in many respects, modeled on that of the United States. The ranking system in the defense forces is similar to that of the U.S. Army, Navy, Air Force, and Marines, and the Presidential Security Service (PSS) performs a role similar to that of the U.S. Secret Service. The National Intelligence Service (NIS) was even known as the Korean Central Intelligence Agency (KCIA) from 1961 to 1981. On the other hand, the police system in the ROK is quite unlike that of the United States.

In addition to an army, navy, air force, and marine corps, the ROK military includes the Homeland Reserve Force. Overseeing the entire military structure are two executive bodies, the National Security Council and the Ministry of Defense. Military intelligence across all branches is the work of the Defense Security Command, formed in 1977 from a merger of the Army Security Command, the Navy Security Unit, and the Air Force Office of Special Investigations.

Though some of these units had names identical to agencies in the U.S. Army, the model for the DSC and its predecessor organizations was the system in Taiwan, or the Republic of China (ROC), where the Guomindang Party had political officers monitoring the military services. The ROK and ROC have similar political histories. Both represent democracy in divided nations whose other portion—North Korea and the People's Republic of China respectively—is communist. Yet both systems were, until near the end of the twentieth century, notorious in the West for the limitations they placed on individual liberties. Both have since experienced liberalization efforts that, in the ROC, led to the end of the one-party Guomindang rule, and in the ROK, reduced the power of the chief intelligence agency.

Created in 1961, KCIA had a mission combining that of the United States CIA and the Federal Bureau of Investigation, though its power in domestic affairs—including virtually unlimited authority to arrest and imprison—was far greater than that of its American counterparts. After KCIA chief Kim Chae-gyu assassinated the dictatorial President Park Chung Hee in 1979, KCIA experienced a purge and loss of power. It emerged in 1981 as the Agency for National Security Planning (ANSP), which still exerted enormous influence. ANSP's role in the 1987 torture and death of student dissident Pak Chong-ch'ol helped spark a move for greater democratization. This ultimately resulted in the 1999 dissolution of ANSP in favor of the National Intelligence Service, which is more clearly subordinated to the national assembly.

In the ROK, there is no local police system; rather, all police are under the authority of the National Police Agency. The latter exerts its authority from the capital in Seoul, where it controls five special-task police agencies, including marine police, and thirteen provincial police headquarters.

FURTHER READING:

BOOKS:

Kim, Jin-hyun, and Chung-in Moon. *Post-Cold War, Democratization, and National Intelligence: A Comparative Perspective.* Seoul: Yonsei University Press, 1996.

ELECTRONIC:

South Korea Intelligence and Security Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/rok/index.html> (March 1, 2003).

SEE ALSO

Japan, Intelligence and Security
North Korean Nuclear Weapons Programs
Korean War
North Korea, Intelligence and Security
Taiwan, Intelligence and Security

Soviet Union (USSR), Intelligence and Security

ALEXANDR IOFFE

On December 20, 1917, less than two months after the October Social Revolution in Russia, the All-Russian Special Commission for Combating Counter-revolution and Sabotage (VChK) was created in the new Soviet Russia. The agency was created by decree of the Council of the People's Commissar (SNK), the government at that time, "for combating counter-revolution and sabotage." The main aim of the commission was the suppression of any opposition to the new regime in any form, and in this case "suppression" very often meant physical extermination of persons who did not approve the regime. In September 1918, the SNK promulgated the decree that came to be known as the "Red Terror." Officially, the red terror was provoked by the increasing activity of the opposition that threatened the emerging Soviet government. The decree served as a basis for purging opposition, however, and punishing perceived enemies of the Soviet power by isolation in concentration or work camps. The VChK began an organized campaign to capture perceived enemies of the state, imprison them, or often, execute them without benefit of a trial.

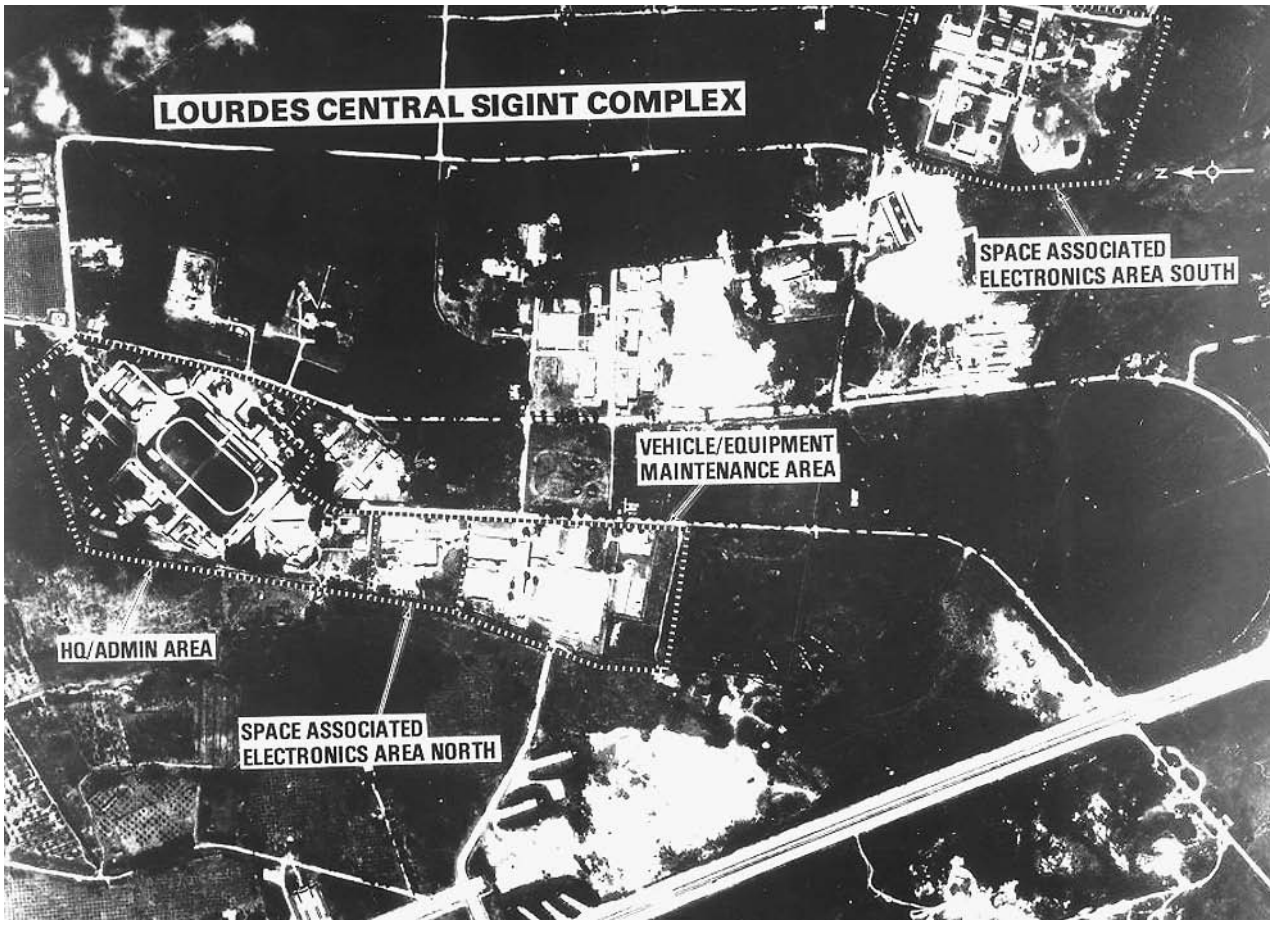
The *Liman*, center, an intelligence-gathering vessel of Russia's Black Sea Fleet, sails through the Bosphorus Strait in 1999 on a mission to gain information about conflicts among the Balkan states. AP/WIDE WORLD PHOTOS.

In February 1922, the VChK was formally abolished, but it was practically reorganized as the State Politic Administration of NKVD, and in November 1923, it was reorganized again as the Joint State Politic Administration (OGPU) of the SNK. Felix Dzerzhinskii, a former professional revolutionary born in Poland, headed these structures until his death in 1926. Compared to the VChK, the OGPU's activities enlarged, as it began to engage not only in problems of internal security of the regime, but also in problems of intelligence and active work abroad. The Foreign Department (INO) was created within the OGPU in December 1920, for the purpose of conducting intelligence and subversive activities in foreign countries. In this work, the OGPU cooperated actively with the Comintern, the Communist International, whose leaders of were in Moscow, and which was under total control of the Communist Party of the Soviet Union.

The People's Commissariat of Home Affairs (NKVD) was also organized in 1917 in Soviet Russia to handle the security concerns of the new regime. The country's police force (officially named "militsia") reported to the NKVD. Functions of the NKVD and successors of the VChK often became entangled, and during the period from the 1920s until the beginning of World War II, these two organizations operated both jointly and separately. In 1934, the new "All-Union" People's Commissariat of Home Affairs (known again as the NKVD) was created. The new NKVD included the Main Agency of State Security (GUGB), which was the successor of the OGPU. The new NKVD also included the central agency of Militsia (police), the border and internal guards, and the fire guards.

A notorious arm of the NKVD was the main agency responsible for labor camps and deportation, the Gulag. Activities of the infamous Gulag were described in detail in the works of the Nobel Prize-winning Soviet dissident and work camp prisoner Alexander Solzhenitsyn. The Gulag interred millions of political prisoners in camps throughout the Soviet Union, and became infamous for its cruel methods of suppression.

From September 1936, until December 1938, the head of the NKVD was Nikolai Ezhov, who became infamous for his efficient cruelty. During this period of purges ordered by the Soviet leader Joseph Stalin and known as the Great Terror, over 1.5 million Soviet citizens were arrested for



The Kremlin learned of U.S. battle plans for the 1991 Persian Gulf War through its electronic spy network based in Cuba and known as Lourdes, seen in this photo taken by a U.S. spy plane. AP/WIDE WORLD PHOTOS.

crimes against the state. Almost half of those arrested were executed by gunfire. Although acting under direct orders from Stalin, this period is often referred to as "Ezhovshina," meaning Ezhov's time. Eventually, Ezhov himself was arrested and executed, as Stalin grew suspicious of Ezhov's knowledge and tactics. Ezhov was replaced by Lavrenti P. Beria, who served as the head of the NKVD, along with other Soviet security agencies until 1953, when Beria was arrested and shot for attempting to gain power after the death of Stalin. The Great Terror continued under Beria, with the numbers interned in the Gulag work camps estimated between 4 and 20 million by the end of 1939.

Also before World War II, Soviet intelligence gave serious attention to suppressing political enemies of the regime. Probably the best-known example of such activity is the assassination of Leon Trotsky, the main political enemy of Stalin and one of the leaders of the Russian Revolution. Trotsky was deported from the USSR in 1929; he roamed from country to country seeking political refuge, finally settling in Mexico. Soviet secret services tried to murder him several times according Stalin's order. At first, the Russians used Mexican communists in the attempts to murder Trotsky. In one such attempt, the famous Mexican painter David Siqueiros participated. A group of Mexicans with machine guns riddled Trotsky's bedroom with bullets one night, then escaped, assuming that Trotsky was dead. Trotsky and his wife, however, were alerted, and hid safely under the bed. After this assassination attempt, Trotsky supporters guarded his home. Finally, the Russian NKVD agent Ramon Merkader befriended Trotsky's secretary, and through her unknowing confidence, gained access to the Trotsky home carrying an ice-axe, and carried out the assassination of on August 20, 1940.

The Komitet Gosudarstvennoy Bezopasnosti (KGB), or Committee for State Security, was the primary organization during the Soviet period for intelligence and counterintelligence matters, although it often played a role in maintaining domestic security alongside the NKVD. In the years of the new Soviet Republic before World War II, some people in Western countries supported communism and cooperated with the KGB for ideological reasons. One famous example of such cooperation is the case

of the "Cambridge five." Soviet intelligence drew upon the sympathies and cooperation of five students at Cambridge University (Kim Philby, Donald McLean, Guy Burgess, John Carincross, and Anthony Blunt) to recruit them as spies in the 1930s. After World War II, several members of the spy ring attained key positions in the British intelligence service, where they gained access to many of Britain's most guarded secrets. Led by Philby, components of the spy ring fed Western intelligence secrets to the Soviets for over a decade after the war. After they were exposed, MacLean and Burgess defected to the Soviet Union in 1949; Philby escaped detection and functioned in his role as double agent until 1963, when he also defected and became a colonel in the KGB. Both Blunt and Carincross escaped detection and remained in Britain until the 1990s, when they were exposed by the British government.

During World War II, the activity of all Soviet intelligence and secret services became much more active; old agent ties were restored and new ones were created. Counter-intelligence and strategic data connected with the war activity were obtained. After the end of the war the "atomic espionage" began. And along with this, the concentration camps continued to exist in the country, and new repressive tasks appeared. Stalin, for example, ordered the exile of entire nations (e.g., the Crimean Tartars, the Chechens), and this order was executed strictly.

Activities of the Soviet secret services remained acute after World War II. In 1954, the famous State Security Committee (KGB) was again created after reorganization, which conducted intelligence and repressive activities along with other information gathering. The head of the KGB enjoyed an important position in the totalitarian regime hierarchy, and one, Yuri Andropov, even became the head of the Soviet state. KGB leaders played an important role in the attempt to overthrow the government of the first (and last) president of the USSR, Mikhail Gorbachev, when they isolated Gorbachev in the Crimea for three days during his vacation in August, 1991.

The KGB was essentially abolished after the failure of the anti-Gorbachev putsch and the collapse of the USSR in 1991. The following agencies were created from within the KGB: the Federal Security Service (FSB); the Federal Agency of Government Intercommunication, which is responsible for communications between top state officials; the Guard Service, which guards top state officials; and the Outer Intelligence Service, which collects and processes all data coming from abroad.

Immediately after the Red (Soviet) Army was created in the early twentieth century, its own intelligence was organized, and by 1917, the Department of Agitation and Intelligence of the General Staff was operational. With the increasing power of the Army, its intelligence strengthened, and before World War II, the Intelligence agency of the Red Army was formally organized in 1934, and later reorganized again into the Main Intelligence Agency (GRU). The Soviet Army Intelligence existed until the collapse of the USSR, and today exists in the Russian Army. In the end of the Soviet epoch, this Agency was the most powerful intelligence structure, and executed different tasks of both strategic and operative intelligence with large networks of agents abroad and representatives in practically in every Soviet embassy. The GRU had its own dedicated troops and unofficially competed with the KGB for power and prestige in the Soviet government.

■ FURTHER READING:

BOOKS:

Janseen, Marc, and Nikita Petrov. *Stalin's Loyal Executioner: People's Commissar Nikolai Ezhov 1895–1940.* Palo Alto, CA: Hoover Institution Press, 2002.

Knight, Amy. *Beria: Stalin's First Lieutenant.* Princeton, NJ: Princeton University Press, 1996.

PERIODICALS:

Waller, Michael J. "State within a State: the KGB and its Successors." *Perspective* IV,4 (1994).

ELECTRONIC:

Federation of American Scientists, FAS Intelligence Resource Program. "Soviet/Russian Intelligence Agencies" <http://www.fas.org/irp/world/russia/> (April 18, 2003).

SEE ALSO

Cold War (1945–1950), The start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
Russia, Intelligence and Security
Russian Nuclear Materials, Security Issues

Space Imaging.

SEE *Satellites, Non-Governmental High Resolution.*

Space Shuttle

Although NASA is a civilian space agency, the United States military has used the space shuttle fleet to carry classified military payloads into space. The Department of Defense (DoD) had generally received priority in scheduling national security related flights. In addition to fully classified missions, the Department of Defense (DoD) has contracted shuttle research time and lifted unclassified early warning satellites into orbit. Satellites deployed from

the shuttle, or serviced by shuttle crews, are used for electronic intelligence, photographic and radar reconnaissance, and defense communications.

By 1990, at least eight classified military satellites were placed in orbit during classified shuttle missions. Although the shuttle fleet is still used for a range of classified missions, following the loss of *Challenger* the military shifted emphasis to launching classified military satellites by expendable rockets.

The Shuttle Program

The space shuttle is a reusable spacecraft that takes off like a rocket, orbits the Earth like a satellite, and then lands like a glider. The space shuttle has been essential to the repair and maintenance of the Hubble Space Telescope and for construction of the International Space Station; it has also been used for a wide variety of other military, scientific, and commercial missions. It is not capable of flight to the Moon or other planets, being designed only to orbit the Earth.

The first shuttle to be launched was the *Columbia*, on April 12, 1981. Since that time, two shuttles have been lost in flight: *Challenger*, which exploded during takeoff on January 28, 1986, and *Columbia*, which broke up during reentry on Feb. 1, 2003. Seven crew members died in each accident. The three remaining shuttles are the *Atlantis*, the *Discovery*, and the *Endeavor*. The first shuttle actually built, the *Enterprise*, was flown in the atmosphere but never equipped for space flight; it is now in the collection of the Smithsonian Museum.

A spacecraft closely resembling the U.S. space shuttle, the Aero-Buran, was launched by the Soviet Union in November, 1988. Buran's computer-piloted first flight was also its last; the program was cut to save money and all copies of the craft that had been built were dismantled.

Mission of the space shuttle. At one time, both the United States and the Soviet Union envisioned complex space programs that included space stations orbiting the Earth and reusable shuttle spacecraft to transport people, equipment, raw materials, and finished products to and from these space stations. Because of the high cost of space flight, however, each nation eventually ended up concentrating on only one aspect of this program. The Soviets built and for many years operated space stations (*Salyut*, 1971–1991, and *Mir*, 1986–2001), while Americans have focused their attention on the space shuttle. The brief Soviet excursion into shuttle design (Buran) and the U.S. experiment with Skylab (1973–1979) were the only exceptions to this pattern.

The U.S. shuttle system—which includes the shuttle vehicle itself, launch boosters, and other components—is officially termed the Space Transportation System (STS). Lacking a space station to which to travel until 1998, when construction of the International Space Station began, the shuttles have for most of their history operated with two major goals: (1) the conduct of scientific experiments in a microgravity environment and (2) the release, capture, repair, and re-release of scientific, commercial, and military satellites. Interplanetary probes such as the Galileo mission to Jupiter (1989–) have been transported to space by the shuttle before launching themselves on interplanetary trajectories with their own rocket systems. Since 1988, the STS has also been essential to the construction and maintenance in orbit of the International Space Station.

One of the most important shuttle missions ever was the repair of the Hubble Space Telescope by the crew of the *Endeavor* in December, 1993 (STS-61). The Hubble had been deployed, by a shuttle mission several years earlier, with a defective mirror; fortunately, it had been designed to be repaired by spacewalking astronauts. The crew of the *Endeavor* latched on to the Hubble with the shuttle's robotic arm, installed a corrective optics package that restored the Hubble to full functionality. The Hubble has since produced a unique wealth of astronomical knowledge.

The STS depends partly on contributions from nations other than the U.S. For example, its Spacelab modules—habitable units, carried in the shuttle's cargo bay, in which astronauts carry out most of their experiments—are designed and built by the European Space Agency, and the extendible arm used to capture and release satellites—the "remote manipulator system" or Canadarm—is constructed in Canada. Nevertheless, the great majority of STS costs continue to be borne by the United States.

Structure of the STS. The STS has four main components: (1) the orbiter (i.e., the shuttle itself), (2) the three main engines integral to the orbiter, (3) the external fuel tank that fuels the orbiter's three engines during liftoff, and (4) two solid-fuel rocket boosters also used during liftoff.

The orbiter. The orbiter, which is manufactured by Rockwell, International, Inc., is approximately the size of a commercial DC-9 jet, with a length of 122 ft (37 m), a wing span of 78 ft (24 m), and a weight of approximately 171,000 lb (77,000 kg). Its interior, apart from the engines and various mechanical and electronic compartments, is subdivided into two main parts: crew cabin and cargo bay.

The crew cabin has two levels. Its upper level—literally "upper" only when the shuttle is in level flight in Earth's atmosphere, as there is no literal "up" and "down" when it is orbiting in free fall—is the flight deck, from which astronauts control the spacecraft during orbit and descent, and its lower level is the crew's personal quarters, which contains personal lockers and sleeping, eating, and toilet facilities. The crew cabin's atmosphere is approximately equivalent to that on the Earth's surface, with a composition 80% nitrogen and 20% oxygen.

The cargo bay is a space 15 ft (4.5 m) wide by 60 ft (18 m) long in which the shuttle's payloads—the modules or satellites that it ports to orbit or back to Earth—are stored. The cargo bay can hold up to about 65,000 lb (30,000 kg) during ascent, and about half that amount during descent.

The shuttle can also carry more habitable space than that in the crew cabin. In 1973, an agreement was reached between the U.S. National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA) for the construction by ESA of a pressurized, habitable workspace that could be carried in the shuttle's cargo bay. This workspace, designated Spacelab, was designed for use as a laboratory in which various science experiments could be conducted. Each of Spacelab module is 13 ft (3.9 m) wide and 8.9 ft (2.7 m) long. Equipment for experiments is arranged in racks along the walls of the Spacelab. The whole module is loaded into the cargo bay of the shuttle prior to take-off, and remains there while the shuttle is in orbit, with the cargo-bay doors opened to give access to space. When necessary, two Spacelab modules can be joined to form a single, larger workspace.

Propulsion systems. The power needed to lift a space shuttle into orbit comes from two solid-fuel rockets, each 12 ft (4 m) wide and 149 ft (45.5 m) long, and from the shuttle's three built-in, liquid-fuel engines. The fuel used in the solid rockets is compounded of aluminum powder, ammonium perchlorate, and a special polymer that binds the other ingredients into a rubbery matrix. This mixture is molded into a long prism with a hollow core that resembles an 11-pointed star in cross section. This shape exposes the maximum possible surface area of burning fuel during launch, increasing combustion efficiency.

The two solid-fuel rockets each contain 1.1 million lb (500,000 kg) at ignition, together produce 6.6 million pounds (29.5 million N) of thrust, and burn out only two minutes after the shuttle leaves the launch pad. At solid-engine burnout, the shuttle is at an altitude of 161,000 ft (47,000 m) and 212 miles (452 km) down range of launch site. (In rocketry, "down range" distance is the horizontal distance, as measured on the ground, that a rocket has traveled since launch, as distinct from the greater distance it has traveled along its actual flight path.) At this point, explosive devices detach the solid-fuel rockets from the shuttle's large, external fuel tank. The rockets return to Earth via parachutes, dropping into the Atlantic Ocean at a speed of 55 miles (90 km) per hour. They can then be collected by ships, returned to their manufacturer (Morton Thiokol Corp.), refurbished and refilled with solid fuel, and used again in a later shuttle launch.

The three liquid-fuel engines built into the shuttle itself have been described as the most efficient engines ever built; at maximum thrust, they achieve 99% combustion efficiency. (This number describes combustion efficiency, not end-use efficiency. As dictated by the laws of physics, less than half of the energy released in combustion can be communicated to the shuttle as kinetic energy, even by an ideal rocket motor.) The shuttle's main engines are fueled by liquid hydrogen and liquid oxygen stored in the external fuel tank (built by Martin Marietta Corp.), which is 27.5 ft (8.4 m) wide and 154 ft (46.2 m) long. The tank itself is actually two tanks—one for liquid oxygen and the other for liquid hydrogen—covered by a single, aerodynamic sheath. The tank is kept cold (below -454°F [-270°C]) to keep its hydrogen and oxygen in their liquid state, and is covered with an insulating layer of stiff foam to keep its contents cold. Liquid hydrogen and liquid oxygen are pumped into the shuttle's three engines through lines 17in (43 cm) in diameter that carry 1,035 gal (3,900 l) of fuel per second. Upon ignition, each of the liquid-fueled engines develops 367,000 lb (1.67 million N) of thrust.

The three main engines turn off at approximately 522 seconds, when the shuttle has reached an altitude of 50 miles (105 km) and is 670 miles (1,426 km) down range of the launch site. At this point, the external fuel tank is also jettisoned. Its fall into the sea is not controlled, however, and it is not recoverable for future use.

Final orbit is achieved by means of two small engines, the Orbital Maneuvering System (OMS) engines located on external pods at the rear of the orbiter's fuselage. The OMS engines are fired first to insert the orbiter into an elliptical orbit with an apogee (highest altitude) of 139 miles (296 km) and a perigee (lowest altitude) of 46 miles (98 km). They are fired again to nudge the shuttle into a final, circular orbit with a radius of 139 miles (296 km). All these figures may vary slightly from mission to mission.

Orbital maneuvers. For making fine adjustments, the spacecraft depends on six small rockets termed vernier jets, two in the nose and four in the OMS pods. These allow small changes in the shuttle's flight path and orientation.

The computer system used aboard the shuttle, which governs all events during takeoff and on which the shuttle's pilots are completely dependent for interacting with its complex control surfaces during the glide back to Earth, is highly redundant. Five identical computers are used, four networked with each other using one computer program, and a fifth operating independently. The four linked computers constantly communicate with each other, testing each other's decisions and deciding when any one (or two or three) are not performing properly and eliminating that computer or computers from the decision-making process. In case all four of the interlinked computers malfunction, decision-making would be turned over automatically to the fifth computer.

This kind of redundancy is built into many essential features of the shuttle. For example, three independent hydraulic systems are available, each with an independent power systems. The failure of one or even two systems does not, therefore, place the shuttle in what its engineers would call a "critical failure mode"—that is,

cause its destruction. Many other components, of course, simply cannot be built redundantly. The failure of a solid-fuel rocket booster during liftoff (as occurred during the *Challenger* mission of 1981) or of the delicate tiles that protect the shuttle from the high temperatures of atmospheric reentry (as occurred during the *Columbia* mission of 2003) can lead to loss of the spacecraft.

Descent. Some of the most difficult design problems faced by shuttle engineers were those involving the reentry process. When the spacecraft has completed its mission in space and is ready to leave orbit, its OMS fires just long enough to slow the shuttle by 200 MPH (320 km/h). This modest change in speed is enough to cause the shuttle to drop out of its orbit and begin its descent to Earth.

When the shuttle reaches the upper atmosphere, significant amounts of atmospheric gases are first encountered. Friction between the shuttle—now traveling at 17,500 MPH (28,000 km/h)—and air molecules causes the spacecraft's outer surface to heat . Eventually, portions of the shuttle's surface reach 3,000°F (1,650°C).

Most materials normally used in aircraft construction would melt or vaporize at these temperatures. It was necessary, therefore, to find a way of protecting the shuttle's interior from this searing heat. NASA decided to use a variety of insulating materials on the shuttle's outer skin. Parts less severely heated during reentry are covered with 2,300 flexible quilts of a silica-glass composite. The more sensitive belly of the shuttle is covered with 25,000 porous insulating tiles, each approximately 6 in (15 cm) square and 5 in (12 cm) thick, made of a silica-borosilicate glass composite.

The portions of the shuttle most severely stressed by heat—the nose and the leading edges of the wings—are coated with an even more resistant material termed carbon-carbon. Carbon-carbon is made by attaching a carbon-fiber cloth to the body of the shuttle and then baking it to convert it to a pure carbon substance. The carbon-carbon is then coated to prevent oxidation (combustion) of the material during descent.

Landing. Once the shuttle reaches the atmosphere, it ceases to operate as a spacecraft and begins to function as a glider. Its flight during descent is entirely unpowered; its movements are controlled by its tail rudder, a large flap beneath the main engines, and elevons (small flaps on its wings). These surfaces allow the shuttle to navigate at forward speeds of thousands of miles per hour while dropping vertically at a rate of some 140 MPH (225 km/h). When the aircraft finally touches down, it is traveling at a speed of about 190 knots (100 m per second), and requires about 1.5 miles (2.5 km) to come to a stop. Shuttles can land at extra-long landing strips at either Edwards Air Force Base in California or the Kennedy Space Center in Florida.

Military shuttle missions and the military spaceplane. Many shuttle missions have been partly or entirely military in nature. Eight military missions—the majority—have been devoted to the deployment of secret military satellites in three categories: signals intelligence (i.e., eavesdropping on radio communications), optical and radar reconnaissance of the Earth, and military communications. All these deployments occurred between 1982 and 1990, after which the military chose to use uncrewed launch rockets for all classified missions. The shuttle has also supported several military experimental missions and nonclassified satellite deployments. One such was the *Discovery* mission (STS-39) launched on April 28, 1991 (STS-39), which carried multi-experiment hardware platforms designed to be released into space then retrieved by the shuttle after having recorded various observations of space conditions. All science aboard STS-39 was related to the Strategic Defense Initiative.

The U.S. military is developing an armed space shuttle system or "military spaceplane" of its own, and says that it intends to deploy such a system by 2012. According to an Air Force status report released in January 2002, "a military spaceplane armed with a variety of weapons payloads (e.g. unitary penetrator, small diameter bombs, etc.) will be able to precisely attack and destroy a considerable number of critical targets while satisfying the requirement for precise weapons (i.e. circular error probable [CEP] of less than or equal to three meters)…. Spaceplanes can support a wide range of military missions including a worldwide precision strike capability; rapid unpredictable reconnaissance; new space control and missile defense capabilities; and both conventional and new tactical spacelift missions that enable augmentation and reconstitution of space assets." The military spaceplane would also enable the military to deploy satellites on short notice. The Air Force envisions a fleet of some 10 spaceplanes stationed in the continental United States as one component of a "Global Strike Task Force" that, it says, will be "capable of striking any target in the world within 24 hours."

The *Challenger* disaster. Disasters have been associated with both the Soviet (now Russian) and American space programs. The first of the two disasters suffered by the shuttle program took place on January 28, 1986, when the external fuel tank of the shuttle *Challenger* exploded only 73 seconds into the flight. All seven astronauts were killed, including high-school teacher Christa McAuliffe, who was flying on the shuttle as part of NASA's public-relations campaign "Teachers in Space," designed to bolster young people's interest in human space flight.

The *Challenger* disaster prompted a comprehensive study to discover its causes. On June 6, 1986, the Presidential Commission appointed to analyze the disaster published its report. The reason for the disaster, said the

commission, was the failure of an O-ring (literally, a flexible O-shaped ring or gasket) in a joint connecting two sections of one of the solid rocket engines. The O-ring ruptured, allowing flames from the rocket's interior to jet out, burning into the external fuel tank and causing it to explode.

As a result of the *Challenger* disaster, many design changes were made. Most of these (254 modifications in all) were made in the orbiter. Another 30 were made in the solid rocket booster, 13 in the external tank, and 24 in the shuttle's main engine. In addition, an escape system was developed that would allow crew members to abandon a shuttle via parachute in case of emergency, and NASA redesigned its launch-abort procedures. Also, NASA was instructed by Congress to reassess its ability to carry out the ambitious program of shuttle launches that it had been planning. The military began reviving its non-shuttle launch options and switched fully to its own boosters for classified satellite launches after 1990.

The STS was essentially shut down for a period of 975 days while NASA carried out the necessary changes and tested its new systems. On September 29, 1988, the first post-*Challenger* mission was launched, STS-26. On that flight, *Discovery* carried NASA's TDRS-C communications satellite into orbit, putting the American STS program back on track once more.

The *Columbia* disaster. Scores of shuttle missions were successfully carried out between the *Challenger*'s successful 1988 mission and February 1, 2003, when disaster struck again. The space shuttle *Columbia* broke up suddenly during re-entry, strewing debris over much of Texas and several other states and killing all seven astronauts on board. At the time of this writing, analysts speculate that the most likely cause of the loss of the spacecraft related to some form of damage to the outer protective layer of heat-resistant tiles or seals that protect the shuttle's interior from the 3,000°F (1,650°C) plasma (superheated gas) that envelops it during reentry. As described earlier, a coating of rigid foam insulation is used to keep the external fuel tank cool; video cameras recording the *Columbia*'s takeoff show that a piece of this foam broke off 80 seconds into the flight and burst against the shuttle's wing at some 510 MPH (821 km/h). Pieces of foam have broken off and struck shuttles during takeoff before, but this was the largest piece ever—at least 2.7 lb (1.2 kg) and the size of a briefcase.

While *Columbia* was in orbit, NASA engineers, who were aware that the foam strike had occurred, analyzed the possibility that it might have caused significant damage to the shuttle, but decided that it could not have: computer simulations seemed to show that the brittle tiles covering the shuttle's essential surfaces would not be severely damaged. In any event, there were no contingency procedures to fix any such damage. The shuttle does not carry spare tiles or means to attach them, nor does it carry gear that would make a spacewalk to the bottom of the shuttle feasible.

NASA officials also insisted that it would not have been possible to fly the shuttle in such a way as to spare the damage surfaces, as the shuttle's path is already designed to minimize heating on reentry.

Regardless of the exact reason, the shuttle's skin was breached, whether by mechanical damage or some other cause, and hot gases formed a jet that caused considerable damage to the left wing from inside. During reentry, the wing began to break up, experiencing greatly increased drag. The autopilot struggled to compensate by firing steering rockets, but could only stabilize the shuttle temporarily.

As this book goes to press, the loss of the *Columbia* has, like the loss of the *Challenger* in 1986, put a temporary stop to shuttle launches. A moratorium on shuttle launches will also have an impact on the International Space Station, which depends on the shuttle to bring it the fuel it needs to stay in orbit and which cannot be completed without components that only the space shuttle can carry. In the wake of the *Columbia* disaster, NASA and other governmental officials worked with an independent panel's review of the accident and sought technical improvements to the STS program that might prevent future problems while, at the same time returning the remaining shuttles to flight status as soon as safely possible.

■ FURTHER READING:

BOOKS:

Barrett, Norman S. *Space Shuttle.* New York: Franklin Watts, 1985.

Curtis, Anthony R. *Space Almanac.* Woodsboro, MD: Arcsoft Publishers, 1990.

Dwiggins, Don. *Flying the Space Shuttles.* New York: Dodd, Mead, 1985.

PERIODICALS:

Barstow, David. "After Liftoff, Uncertainty and Guesswork." *New York Times.* (February 17, 2003).

Broad, William J. "Outside Space Experts Focusing on Blow to Shuttle Wing." *New York Times.* (February 15, 2003).

Chang, Kenneth. "Columbia Was Beyond Any Help, Officials Say." *New York Times.* (February 4, 2003).

———. "Disagreement Emerges over Foam on Shuttle Tank." *New York Times.* (February 21, 2003).

Seltzer, Richard J. "Faulty Joint behind Space Shuttle Disaster." *Chemical & Engineering News* (23 June 1986): 9–15.

ELECTRONIC:

Space and Missile Systems Center (SMC), United States Air Force. "The Military Space Plane: Providing Transformational and Responsive Global Precision Striking Power." Jan. 17, 2002. <http://www.spaceref.com/news/viewsr.html?pid=4523> (Feb. 17, 2003).

SEE ALSO

NASA (National Air and Space Administration)
Near Space Environment
Satellites, Non-Governmental High Resolution
Satellites, Spy

Spain, Intelligence and Security

Spain is one of the few Western countries in which a single agency handles both internal and external intelligence. This is CNI, or Centro Nacional de Inteligencia (National Intelligence Center). In addition to CNI, the Spanish military and interior ministry each have their own intelligence branches, whose work includes monitoring Basque terrorists.

CNI. From the end of the Spanish Civil War in 1939 until 1975, Spain was under the right-wing dictatorship of Generalissimo Francisco Franco. Following Franco's death, the country liberalized rapidly, and in 1977 it dissolved the old intelligence services that Franco had used to maintain control of the country. In place of the Franco-era Political-Social Brigade, the Spanish government established the Centro Superior de Informacion de la Defensa (CESID or Higher Defense Intelligence Center). CESID in 2001 became CNI.

Nominally a civilian agency, though headed by military personnel, CESID placed a priority on monitoring both the homeland and outlying territories, including the Spanish-owned enclaves of Ceuta and Melilla on the Moroccan coast. It also maintained close relations not only with the intelligence services of Arab countries in North Africa and the Middle East, but with Israel's Mossad as well.

Ministry of Interior. Whereas CNI is primarily concerned with intelligence, the principal focus of the interior ministry is security. The Ministry of Interior is divided into three groups: the National Police, who conduct investigations nationwide and maintain security in urban areas; the Civil Guard, which patrols rural areas, borders, and highways; and autonomous police forces, which have replaced the Civil Guard in Galicia, Catalonia, and the Basque Country.

The last of these regions was the site of the greatest threat to domestic security, in the form of ETA (Euzkadi Ta Azkatasuna or Basque Homeland and Liberty), the separatist organization that claimed to represent the Basque people of northwestern Spain. A right-wing force known as GAL (Grupo Antiterrorista de Liberacion or Antiterrorist Liberation Group), believed by some observers to be composed of Civil Guard members, conducted reprisals against ETA.

In May 2002, Spain's parliament passed a law to create an intelligence and security coordinating committee which would oversee the activities of CNI, the police, and the national guard.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

PERIODICALS:

Champion, Marc. "How Do Other Countries Coordinate Security?" *Wall Street Journal.* (June 12, 2002): A14.

ELECTRONIC:

Spain—Intelligence Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/spain/index.html> (March 1, 2003).

SEE ALSO

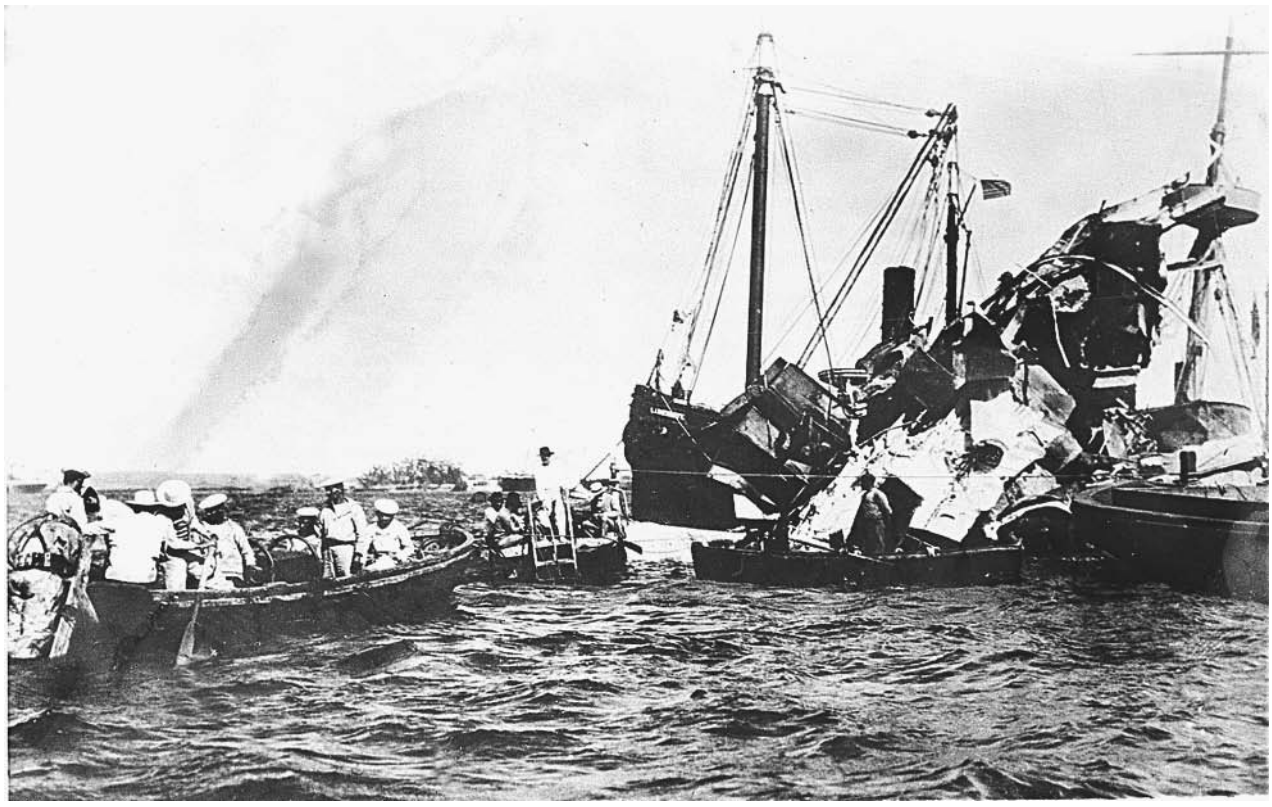
Italy, Intelligence and Security
Morocco, Intelligence and Security
Spanish-American War

Spanish-American War

ADRIENNE WILMOTH LERNER

In the late nineteenth century, the United States grew in industrial and economic strength. By the 1880s, the nation was one of the most robust in the Western Hemisphere, wielding increasing power in the region despite a stated policy of neutrality. In 1898, diplomatic relations between the United States and Spain began to sour over Spain's domination of Latin America and some parts of the Caribbean. Reports of the brutal rule of Spanish General Valeriano Wyler in Cuba inflamed public opinion in the United States. The convergence of anti-Spanish public opinion and the government's desire to protect American economic interests in Cuba prompted tense diplomatic meetings between Spain and the United States.

During the negotiations, two events spurred the United States to declare war. A U.S. ship, the USS *Maine* sank off the coast of Cuba on February 15, 1898. A Navy inquiry board incorrectly declared that a mine fatally wounded the



Lifeboats rescue surviving crewmen of the wrecked USS *Maine* anchored in Havana, Cuba, after an explosion destroyed the battleship in 1898, serving as the catalyst for the outbreak of the Spanish-American War. AP/WIDE WORLD PHOTOS.

vessel. 266 Navy seamen and two high-ranking officers perished in the accident. The event consumed newspaper headlines for weeks. Sensationalistic reporting, dubbed "yellow journalism," helped to swell the tide of pro-war sentiment in the United States.

Within weeks of the sinking of the *Maine*, intelligence operatives intercepted a private letter between the Spanish Ambassador to the United States and a friend in Havana, Cuba. The letter disparaged U.S. President McKinley, and hinted at plans to commit acts of sabotage against American property in Cuba. The letter was published by several newspapers, further agitating public opinion. On April 19, 1898, Congress resolved to end Spanish rule in Cuba.

In the first military action of the war, the United States blockaded Cuban ports on April 22, 1898. The Navy transferred several vessels to neighboring Florida to consolidate the forces available to fight the Spanish in the Caribbean. Naval presence off the Florida coast also facilitated the transfer of information from the battlefront to the government in Washington, D.C.

The Office of Naval Intelligence established sophisticated communications intelligence operations in support of their efforts in Cuba. Martin Hellings, who worked for the International Ocean Telegraph Company, was sent to Key West, Florida, to intercept Spanish messages. Hellings convinced other telegraph operators to copy Spanish diplomatic messages and deliver the copies to him. Within a few days, he operated a sizable communications ring, conducting surveillance on underwater and land-based telegraph cables. Hellings also employed a courier to run special messages between his offices and United States ships in the region.

The theater of war rapidly expanded to include other Spanish strongholds, including the Philippines. Intelligence operations were not initially as well developed in the Pacific as they were in the region around Cuba. Cuba's proximity to the Florida coast aided intelligence and espionage operations. United States military commanders knew little about the Philippines and the Spanish defenses there. To obtain information, the Office of Navy Intelligence and the Army's Military Intelligence Division employed human intelligence. Agents were sent to the remote islands to obtain information about Spanish defenses, military strength, and island terrain. The operation moved swiftly, and within weeks, United States commanders learned that the Spanish were ill-prepared to fight a strong offensive in the Philippines.

On May 1, 1898, the United States Asiatic Squadron, under the command of George Dewey, sailed into Manila Bay and attacked the Spanish. The Spanish fleet was decimated, but the United States sustained no losses.

Though the Spanish surrendered the Philippines, the United States fleet remained, and began a campaign to take the island as a United States territory. The ensuing conflict lasted until 1914.

Human intelligence was not limited to operations in the Philippines. The United States employed covert agents in Europe, Cuba, and Canada. These agents aided the war effort by spying on Spanish diplomats abroad and providing intelligence information to dissident groups in Cuba. German-educated Henry Ward traveled to Spain in the guise of a German physician. William Sims, an American attaché in Paris, managed a spy ring throughout the Mediterranean. In Cuba, Andrew Rowan united rebel groups and reported on the location and size of the Spanish fleet. He supervised the trafficking of arms to rebel outfits and helped plan their assaults on Spanish targets. Human intelligence also contributed to counterintelligence efforts. Based on agent reports, the United States Secret Service was able to infiltrate and destroy a Spanish spy ring working in Montreal, Canada.

In June 1898 United States intelligence learned, via telegraph intercepts, that the Spanish fleet planned to attack the U.S. blockade in Cuba and draw ships into a naval battle in the Caribbean. When the Spanish fleet arrived in the region, United States Naval Intelligence tracked them and gave chase. United States commanders hoped to deplete Spanish fuel reserves before engaging them in battle. The United States backed off, and redeployed to aid blockade ships stationed around Havana. The Spanish ships proceeded undetected to the narrow harbor of Santiago, Cuba. When the Spanish commander telegraphed his government to declare his position, U.S. agents working in Florida intercepted the cable. The United States fleet moved to intercept the Spanish at Santiago. The U.S. Navy blockaded the port and immobilized the Spanish fleet. The Spanish attempted to run the blockade on July 3, but the entire fleet of six ships was destroyed.

In the final phase of the war, the United States deployed ground forces to sweep Spanish forces out of Havana and Santiago. The "Rough Riders," the most famous of which was Theodore Roosevelt, worked with rebel groups to take control of the nation's capitol and ferret out remaining Spanish forces in the countryside. The U.S. troops then departed Cuba for Puerto Rico, driving the Spanish from the island.

The war ended with the Spanish surrender on July 17, 1898. The event signaled a new international stance for the United States, as the nation began to acquire territories and dominate the politics of the Western Hemisphere. As a result of the Spanish-American War, or in its immediate wake, the United States gained Guantanamo Bay, Puerto Rico, Guam, and Hawaii.

The Spanish-American War, though a brief conflict, helped to revolutionize United States intelligence organizations and their operations. Before the war, agencies like the Office of Naval Intelligence relied on openly available sources for their information. After the war, personnel were trained in espionage tradecraft, and covert operations became standard intelligence community practice. Congress briefly entertained the idea of establishing a permanent, civilian intelligence corps, but the agency never materialized. Despite the progress made with technological surveillance, espionage tradecraft, and interagency cooperation made during the war, the intelligence community was once again allowed to slip into disarray until the eve of World War I.

FURTHER READING:

BOOKS:

Musicant, Ivan. *Empire by Default: The Spanish-American War and the Dawn of the American Century.* Henry Holt, 1998.

O'Toole, G. J. A. *The Spanish-American War: An American Epic, 1898.* New York: W.W. Norton, 1986.

SEE ALSO

Monroe Doctrine

Special Collection Service, United States

The National Security Agency (NSA) has a reputation as the most secretive major component of the United States intelligence community, but it is a veritable open book in comparison to one of its subsidiary organizations, the Special Collection Service (SCS). The latter is known to be engaged in communications intelligence (COMINT), primarily in hostile countries, and its personnel appears to include both NSA and Central Intelligence Agency (CIA) operatives.

So secretive that it is sometimes jokingly called "No Such Agency," NSA is home to an even more obscure group, the Central Security Service (CSS). Established in 1972 to provide information security to U.S. communications and crack other nations' codes and ciphers, CSS has within it—like a nesting matryoshka doll—the still more elite and clandestine SCS. Composed primarily of NSA specialists, SCS operatives typically use diplomatic cover in order to put in place eavesdropping equipment in areas where access to U.S. intelligence by less laborious means would be considerably more difficult.

In 1999, one United Nations Special Commission (UNSCOM) weapons inspector claimed that SCS had installed in-country radio relays for UNSCOM that greatly

extended U.S. listening capabilities in Iraq. One of the few references to SCS by federal government sources was the affidavit in the 2001 case of accused spy Robert Hanssen, who was alleged to have provided the Russians with information about the organization.

FURTHER READING:

BOOKS:

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War through the Dawn of a New Century.* New York: Doubleday, 2001.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

ELECTRONIC:

National Security Agency. <http://www.nsa.gov/> (March 24, 2003).

Special Collection Service. Federation of American Scientists. <http://www.fas.org/irp/agency/scs/> (April 2, 2003).

SEE ALSO

COMINT (Communications Intelligence)
Echelon
Information Warfare
NSA (United States National Security Agency)
Satellites, Spy
SIGINT (Signals Intelligence)

Special Counsel and Security Related "Whistleblower" Protection Issues, United States Office

JUDSON KNIGHT

In 1989, the United States Congress passed the Whistleblower Protection Act, which provided protections for federal employees who reported wrongdoing, including theft and fraud, in the workplace. Since that time, several high-profile cases have involved personnel claiming protection through the Office of Special Counsel (OSC), established by that Act. Several federal intelligence agencies, however, are exempt from the whistleblower statute. As a result of reorganizations in airport security following the September 2001, terrorist attacks, whistleblower protections also do not extend to some airport personnel.

Whistleblower provisions. Acts of malfeasance reported to the OSC Disclosure Unit (DU) fall into five general categories: violations of laws, rules, or regulations; gross mismanagement; waste of funds; abuse of authority; and specific danger to public health and safety. The Whistleblower Protection Act (5 U.S.C. 1213) put in place a system unique among existing governmental whistleblower measures. Provisions of the Act protected the confidentiality of the whistleblower, gave the OSC authority to direct an agency head to investigate charges, and compelled the OSC to provide reports on all whistleblower investigations to the president and the appropriate congressional committees.

Transportation Undersecretary John Magaw speaks during a press conference at the Federal Aviation Administration in Washington, where he discussed an agreement to better protect aviation safety agency whistleblowers against reprisals in the era of terrorist threats. AP/WIDE WORLD PHOTOS.

The statute had several caveats, however. Among these was a provision whereby, if the Special Counsel determined that it was necessary to do so, the identity of the whistleblower could be disclosed without his or her consent. Additionally, the law exempted the Federal Bureau of Investigation (FBI), Central Intelligence Agency, and National Security Agency from whistleblower investigations.

The whistleblower statute in practice. A law accompanying the whistleblower statute required the president to establish a separate system to protect FBI whistleblowers, and

after a lawsuit filed by the FBI's Frederic Whitehurst in April 1997, President William J. Clinton instructed Attorney General Janet Reno to create such a system. Eighteen months later, no such system was in place, prompting a lawsuit against the federal government by several FBI employees. Among these was Cheryl Whitehurst, who claimed that she had been the target of harassment due to the whistleblowing report of her husband, a respected explosives residue analyst who charged wrongdoing at the laboratory where he worked.

Other notable whistleblower cases have involved Immigration and Naturalization Service official Neil Jacobs in 1998, Centers for Disease Control branch chief William C. Reeves in 1999, and Army Corps of Engineers economist Donald C. Sweeney II in 2000. In contrast to these federal employees, whose whistleblower rights were never in question, federal airport baggage screeners are not covered by the whistleblower statute.

After consultation with the OSC, the newly created Transportation Security Administration (TSA) determined that a whistleblower action could shut down security operations at an airport, creating an unacceptable situation for an already overtaxed air transportation infrastructure. The law creating the TSA, passed by Congress in November 2001, had given its director broad authority for hiring and firing, and in February 2002, TSA chief John W. Magaw elected to use this power to exempt a portion of his agency from the whistleblower statute.

FURTHER READING:

PERIODICALS:

Barr, Stephen. "Probe's Findings Support INS Whistleblower." *Washington Post.* (December 16, 1998): A29.

Grunwald, Michael. "Former FBI Workers File Whistleblower Suit." *Washington Post.* (October 20, 1998): A17.

———. "Agency Says Engineers Likely Broke Rules." *Washington Post.* (February 29, 2000): A4.

Schneider, Greg. "No Whistleblowing Protections for Airport Baggage Screeners." *Washington Post.* (February 8, 2002): A29.

Stephens, Joe, and Valerie Strauss. "Retaliation Alleged at CDC; Scientist Disclosed Diversion of Funds." *Washington Post.* (August 6, 1999): A19.

ELECTRONIC:

Whistleblower Disclosures. U.S. Office of Special Counsel. <http://www.osc.gov/wbdisc.htm> (April 2, 2003).

SEE ALSO

Airline Security
Civil Aviation Security, United States
FBI (United States Federal Bureau of Investigation)
Intelligence, United States Congressional Oversight
President of the United States (Executive Command and control of Intelligence Agencies)

Special Operations Command, United States

Special operations forces (SOFs) are elite units of the United States military services that are used for purposes that include counterterrorism, asymmetric warfare, forward reconnaissance, and preparation for landing by airborne and conventional troops in a combat zone. Though some such units have existed since World War II, the formal organization of special operations did not emerge until much later, culminating in the establishment of the U.S. Special Operations Command (SOCOM) on April 16, 1987. Headquartered at MacDill Air Force Base in Florida, SOCOM brings together special operations units and closely related support groups, including psychological warfare contingents, under a single unified command.

SOCOM is one of the nine unified commands of the U.S. Department of Defense (DOD), and its commander-in-chief (USCINCSOC), a four-star general, is the only unified command leader with authority to make purchases in support of his troops. The SOCOM budget for fiscal year 2002 was $4.9 billion, well over 1 percent of DoD appropriations. In September 2002, after Defense Secretary Donald Rumsfeld called for increased SOF involvement in the war on terror, USCINCSOC General Charles Holland presented him with a five-year budget that would double funding for SOCOM.

Components of SOCOM include the U.S. Army Special Operations Command, Joint Special Operations Command, and John F. Kennedy Special Warfare Center and School, all located at Fort Bragg, North Carolina; the Air Force Special Operations Command and Special Operations School at Hurlburt Field, Florida; and the Naval Special Warfare Command and Special Warfare Center at Coronado, California. Among the many elite units that make up SOCOM are the U.S. Army Rangers, Special Forces ("Green Berets"), and Delta Force; the Navy SEALs (sea, air, land); and various Air Force special operations groups.

FURTHER READING:

BOOKS:

Bohrer, David. *America's Special Forces.* St. Paul, MN: MBI Publishing, 2002.

Clancy, Tom, and John Gresham. *Special Forces: A Guided Tour of U.S. Army Special Forces.* New York: Berkley Books, 2001.

Clancy, Tom, Tony Koltz, and Carl Stiner. *Shadow Warriors: Inside the Special Forces.* New York: G.P. Putnam's Sons, 2002.

PERIODICALS:

Wall, Robert. "Conflict Could Test Special Ops Improvements." *Aviation Week & Space Technology* 155, no. 14 (October 1, 2001): 30–31.

ELECTRONIC:

Special Operations.com. <http://www.specialoperations.com/> (April 2, 2003).

U.S. Air Force Special Operations Command. <http://www.afsoc.af.mil/> (April 2, 2003).

U.S. Army Special Operations Command. <http://www.soc.mil/> (April 2, 2003).

U.S. Army Special Operations Command. <http://www.bragg.army.mil/18abn/usa_special_operations_command.htm> (April 2, 2003).

SEE ALSO

Asymmetric Warfare
Delta Force
DoD (United States Department of Defense)
Guerilla Warfare
SEAL Teams
United States, Counter-terrorism Policy

Special Relationship: Technology Sharing between the Intelligence Agencies of the United States and United Kingdom

JUDSON KNIGHT

During World War II, the intelligence services of the United States and the United Kingdom worked together in their efforts against the Axis powers, particularly in Europe, and formalized the collaboration with agreements in 1943 and 1946. Only in the postwar era did the United States emerge as the dominant partner, and even then, many of the most important technological advances in intelligence came from Britain. Among the most visible examples of U.S.-British cooperation in the early twenty-first century were joint military efforts in Afghanistan and Iraq. Behind these undertakings lay a more extensive framework of cooperation in intelligence, whose most significant known component is the Echelon global surveillance system.

U.S. and British relations through 1945. Great Britain is one of the only nations, other than Germany, against which Americans have fought twice: first in the Revolutionary War (1775–83), and later in the War of 1812. A century later, the two nations allied against the Central Powers in World War I. The "special relationship" between the Anglo-American powers only became apparent in World War II, when Italy and Russia signed pacts with the Nazis, and France readily capitulated to them. With Britain the only European nation opposing Hitler, the United States—which did not enter the war until two years after it began in Europe—transferred considerable war materiel to the United Kingdom through the Lend-Lease program.

At that time, Britain, with its vast empire, was still perceived as the greater of the two powers, and in many regards, it maintained the lead. Despite the legendary status that wartime U.S. intelligence efforts have gained in retrospect, it was the British who scored the single greatest intelligence breakthrough of the war: Ultra, the successful effort to decipher German radio transmissions made with the Enigma machine. This in turn gave the Allies an enormous advantage over the Germans, who only learned—along with the rest of the world—about Ultra long after the war was over.

Certainly the Soviets did not know about Ultra, or any number of other secrets maintained by the democratic portion of the allied force. In a stroke of good fortune for the postwar world, the instincts of the anticommunist British prime minister, Winston Churchill, prevailed over the desire of U.S. president Franklin D. Roosevelt to share information equitably, and the two countries withheld the most sensitive information from the Soviets. Dictator Josef Stalin did not even known about plans for the Normandy invasion almost until the launch of the attack in June 1944.

Formal agreements and technology-sharing. Midway of the war, the United States and United Kingdom formalized their special relationship with the British-United States Agreement (Brusa) of May 17, 1943. Brusa put into writing what had already existed in fact: virtually complete sharing of signals intelligence. As members of the British Empire, Australia and Canada—which also participated in the Normandy invasion—later also signed on to the agreement.

These four nations, along with New Zealand, became parties to the United Kingdom-United States of America Security Agreement, known as UKUSA, signed on March 5, 1946. UKUSA greatly extended the provisions of Brusa, allowing for standardized terminology, techniques, and procedures. After 1947, the U.S. National Security Agency took the lead in UKUSA, around which grew the vast intelligence-gathering network known as Echelon. Only in the late 1990s did Echelon become public knowledge.

Throughout much of the period before and during World War II, and for several decades thereafter, Great

Britain played a powerful role in the technological dimension of this arrangement. The British had, if not the lead, at least a position of parity with the Americans where technological advances were concerned. Particularly notable were the many advances they made in the technology of naval warfare, both for aircraft carriers and the planes associated with them. One outstanding example of this is the British Harrier jet, whose unusual ability to hover made it an ideal craft for the U.S. Marines.

America's closest friend. In the years since Vietnam, as anti-Americanism took hold in much of western Europe and the developing world, Britain distinguished itself by its virtually unfailing support for the United States. This became particularly apparent following the September 11, 2001, terrorist attacks on the United States. The United Kingdom made this support concrete, first in the war against the Taliban regime in Afghanistan, and later against Saddam Hussein's dictatorship in Iraq. (Australia, too, supported the United States with troops in both efforts, while Canada provided troops for the Afghanistan war.) At the same time, British technological advances remained a vital aspect of the partnership: in October 2002, for instance, the U.S. General Services Administration awarded a contract to British software developer Autonomy for a system to used in tracking suspected terrorists.

FURTHER READING:

Aldrich, Richard J. *Intelligence and the War against Japan: Britain, America, and the Politics of Secret Service.* New York: Cambridge University Press, 2000.

———. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence.* Woodstock, NY: Overlook Press, 2002.

Richelson, Jeffrey. *The Ties that Bind: Intelligence Cooperation between the UKUSA Countries.* Boston: Unwin Hyman, 1990.

Whiting, Charles. *The Spymasters: The True Story of Anglo-American Intelligence Operations within Nazi Germany, 1939–1945.* New York: Saturday Review Press, 1976.

PERIODICALS:

Chapman, Gary. "U.S.-British Cyber-Spy System Puts European Countries on Edge." *Los Angeles Times.* (August 16, 1999): 3.

Markoff, John. "British Concern to Help U.S. Track Terrorists." *New York Times.* (October 12, 2002): A8.

SEE ALSO

Aircraft Carrier
Enduring Freedom, Operation
Enigma
Iraqi Freedom, Operation (2003 War Against Iraq)
United Kingdom, Intelligence and Security

Spectroscopy

JULI BERWALD

Spectroscopy is the measurement of the absorption, scattering, or emission of electromagnetic radiation by atoms or molecules. Absorption is the transfer of electromagnetic energy from a source to an atom or molecule. Scattering is the redirection of light as a result of its interaction with matter. Emission is the transition of electromagnetic energy from a one energy level to another energy level that results in the emission of a photon.

When atoms or molecules absorb electromagnetic energy, the incoming energy transfers the quantized atomic or molecular system to a higher energy level. Electrons are promoted to higher orbitals by ultraviolet or visible light; vibrations are excited by infrared light, and rotations are excited by microwaves. Atomic-absorption spectroscopy measures the concentration of an element in a sample, whereas atomic-emission spectroscopy aims at measuring the concentration of elements in samples. UV-VIS absorption spectroscopy is used to obtain qualitative information from the electronic absorption spectrum, or to measure the concentration of an analyte molecule in solution. Molecular fluorescence spectroscopy is a technique for obtaining qualitative information from the electronic fluorescence spectrum, or for measuring the concentration of an analyte in solution.

Infrared spectroscopy has been widely used in the study of surfaces. The most frequently used portion of the infrared spectrum is the region where molecular vibrational frequencies occur. This technique was first applied around the turn of the twentieth century in an attempt to distinguish water of crystallization from water of constitution in solids.

Ultraviolet spectroscopy takes advantage of the selective absorbance of ultraviolet radiation by various substances. The technique is especially useful in investigating biologically active substances such as compounds in body fluids, and drugs and narcotics either in the living body (*in vivo*) or outside it (*in vitro*). Ultraviolet instruments have also been used to monitor air and water pollution, to analyze dyestuffs, to study carcinogens, to identify food additives, to analyze petroleum fractions, and to analyze pesticide residues. Ultraviolet photoelectron spectroscopy, a technique that is analogous to x-ray photoelectron spectroscopy, has been used to study valence electrons in gases.

Microwave spectroscopy, or molecular rotational resonance spectroscopy, addresses the microwave region of the electromagnetic spectrum and the absorption of energy by molecules as they undergo transitions between rotational energy levels. From these spectra, it is possible to obtain information about molecular structure, including bond distances and bond angles. One example of the application of this technique is in the distinction of trans

and gauche rotational isomers. It is also possible to determine dipole moments and molecular collision rates from these spectra.

In nuclear magnetic resonance (NMR), resonant energy is transferred between a radio-frequency alternating magnetic field and a nucleus placed in a field sufficiently strong to decouple the nuclear spin from the influence of atomic electrons. Transitions induced between substrates correspond to different quantized orientations of the nuclear spin relative to the direction of the magnetic field. Nuclear magnetic resonance spectroscopy has two subfields: broadline NMR and high resolution NMR. High resolution NMR has been used in inorganic and organic chemistry to measure subtle electronic effects, to determine structure, to study chemical reactions, and to follow the motion of molecules or groups of atoms within molecules.

Electron paramagnetic resonance is a spectroscopic technique similar to nuclear magnetic resonance except that microwave radiation is employed instead of radio frequencies. Electron paramagnetic resonance has been used extensively to study paramagnetic species present on various solid surfaces. These species may be metal ions, surface defects, or adsorbed molecules or ions with one or more unpaired electrons. This technique also provides a basis for determining the bonding characteristics and orientation of a surface complex. Because the technique can be used with low concentrations of active sites, it has proven valuable in studies of oxidation states.

Atoms or molecules that have been excited to high energy levels can decay to lower levels by emitting radiation. For atoms excited by light energy, the emission is referred to as atomic fluorescence; for atoms excited by higher energies, the emission is called atomic or optical emission. In the case of molecules, the emission is called fluorescence if the transition occurs between states of the same spin, and phosphorescence if the transition takes place between states of different spin.

In x-ray fluorescence, the term refers to the characteristic x-rays emitted as a result of absorption of x-rays of higher frequency. In electron fluorescence, the emission of electromagnetic radiation occurs as a consequence of the absorption of energy from radiation (either electromagnetic or particulate), provided the emission continues only as long as the stimulus producing it is maintained.

The effects governing x-ray photoelectron spectroscopy were first explained by Albert Einstein in 1905, who showed that the energy of an electron ejected in photoemission was equal to the difference between the photon and the binding energy of the electron in the target. In the 1950s, researchers began measuring binding energies of core electrons by x-ray photoemission. The discovery that these binding energies could vary as much as 6 eV, depending on the chemical state of the atom, led to rapid development of x-ray photoelectron spectroscopy, also known as Electron Spectroscopy for Chemical Analysis (ESCA). This technique has provided valuable information about chemical effects at surfaces. Unlike other spectroscopies in which the absorption, emission, or scattering of radiation is interpreted as a function of energy, photoelectron spectroscopy measures the kinetic energy of the electrons(s) ejected by x-ray radiation.

Mössbauer spectroscopy was invented in the late 1950s by Rudolf Mössbauer, who discovered that when solids emit and absorb gamma rays, the nuclear energy levels can be separated to one part in 10^{14}, which is sufficient to reflect the weak interaction of the nucleus with surrounding electrons. The Mössbauer effect probes the binding, charge distribution and symmetry, and magnetic ordering around an atom in a solid matrix. An example of the Mössbsauer effect involves the Fe^{57} nuclei (the absorber) in a sample to be studied. From the ground state, the Fe^{57} nuclei can be promoted to their first excited state by absorbing a 14.4-keV gamma-ray photon produced by a radioactive parent, in this case Co^{57}. The excited Fe^{57} nucleus then decays to the ground state via electron or gamma ray emission. Classically, one would expect the Fe^{57} nuclei to undergo recoil when emitting or absorbing a gamma-ray photon (somewhat like what a person leaping from a boat to a dock observes when his boat recoils into the lake); but according to quantum mechanics, there is also a reasonable possibility that there will be no recoil (as if the boat were embedded in ice when the leap occurred).

When electromagnetic radiation passes through matter, most of the radiation continues along its original path, but a tiny amount is scattered in other directions. Light that is scattered without a change in energy is called Rayleigh scattering; light that is scattered in transparent solids with a transfer of energy to the solid is called Brillouin scattering. Light scattering accompanied by vibrations in molecules or in the optical region in solids is called Raman scattering.

In vibrational spectroscopy, also known as Raman spectroscopy, the light scattered from a gas, liquid, or solid is accompanied by a shift in wavelength from that of the incident radiation. The effect was discovered by the Indian physicist C. V. Raman in 1928. The Raman effect arises from the inelastic scattering of radiation in the visible region by molecules. Raman spectroscopy is similar to infrared spectroscopy in its ability to provide detailed information about molecular structures. Before the 1940s, Raman spectroscopy was the method of choice in molecular structure determinations, but since that time infrared measurements have largely supplemented it. Infrared absorption requires that a vibration change the dipole moment of a molecule, but Raman spectroscopy is associated with the change in polarizability that accompanies a vibration. As a consequence, Raman spectroscopy provides information about molecular vibrations that is particularly well suited to the structural analysis of covalently bonded molecules, and to a lesser extent, of ionic crystals. Raman spectroscopy is also particularly useful in studying

the structure of polyatomic molecules. By comparing spectra of a large number of compounds, chemists have been able to identify characteristic frequencies of molecular groups, e.g., methyl, carbonyl, and hydroxyl groups.

Spectroscopy has great potential to enhance military and defense capabilities. Both chemical and biological warfare agents are detectable, and potentially identifiable, by spectroscopic imaging. New technology involving fiber optic systems and lasers that can quickly change frequencies provides the opportunity to miniaturize spectroscopic equipment. Systems are currently being developed, which will take this technology into the battlefield in order to target surface and ground contamination by chemical and biological weapons. Spectroscopic examination can also aid in the identification and measurement of subcellular processes, such as carbon dioxide production or oxygen use. These measurements facilitate the understanding of cell growth, cellular response to environmental stimuli, and cellular reactions to drugs and biological and chemical warfare agents.

FURTHER READING:

PERIODICALS:

Behnisch, P.A. "Biodetectors in Environmental Chemistry: Are We at a Turning Point?" *Environ Int* 27(2001):441–42.

"Early Warning Technology." *Med Device Technol* 13 (2002): 70–72.

Casagrande R. "Technology against Terror." *Scientific American.* 287 (2002):59–65.

ELECTRONIC:

Scripps Center for Mass Spectrometry (BC-007), 10550 North Torrey Pines Rd., La Jolla, CA 92037. (858) 784–9596. Gary Suizdak, director. <http://masspec.scripps.edu/information/intro/index.html.> (January 5, 2003).

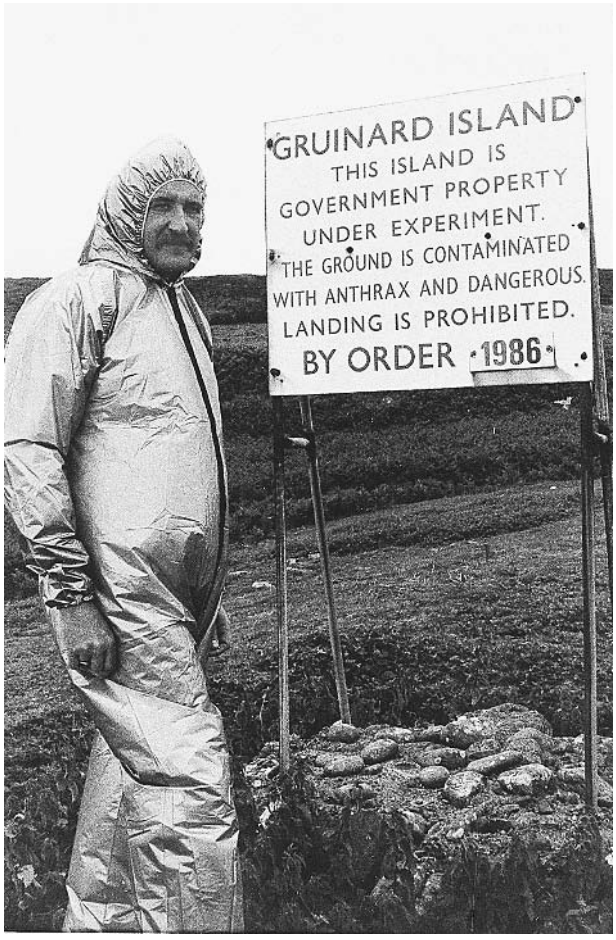
SEE ALSO

Biological Warfare, Advanced Diagnostics
Biomedical Technologies
Chemical and Biological Detection Technologies
Electromagnetic Spectrum
Electromagnetic Weapons, Biochemical Effects
Microscopes

Spores

BRIAN HOYLE

A spore is a hard casing that contains the genetic material of those bacteria and other microorganisms that are able to form the structure. This physically and chemically resilient package protects the genetic material during periods when the environmental conditions are so harsh that the growing form of the microbe would be killed.



A member of the Ministry of Defense Chemical Defense Establishment stands near a warning sign in Gruinard Island, Scotland, the site of explosive munitions testing using anthrax spores as a biological weapon. The island was sealed off from the public for almost 50 years. AP/WIDE WORLD PHOTOS.

The effect of temperature on bacterial and spore survival provides a good example of the resilience of bacterial spores. Temperatures of 80 to 90° Celsius (176–194°F) typically kill bacteria that are growing and dividing within minutes. These high temperatures cause structural components of the bacteria to dissolve, and strands of genetic material to separate from one another. A group of bacteria known as thermophilic bacteria can survive these temperatures, but temperatures of 120°C (248°F) kill even thermophiles. In contrast, spores can survive exposure to 120°C for several hours.

Spores of bacteria that subsequently could be revived into the growing form have been recovered from materials that are over a century old. Thus, spores offer an extraordinary form of protection to bacteria. Anthrax spores that could germinate into living bacteria were recovered on Gruinard Island, an island off the coast of Scotland that

was used for biological weapons testing by the British government during World War II.

Spores are noteworthy in terms of security because of the threat they pose in the hands of terrorists. *Bacillus anthracis*, the bacterium that causes anthrax, is a spore former. The spores are very light and tiny. As a result, they can be readily dispersed through the air and can be easily inhaled into the lungs. The resulting lung infection, which is called inhalation anthrax, is almost always fatal without prompt medical treatment. Anthrax spores were used as a mechanism of bioterrorism to target United States citizens by deliberate dispersal in the mail system in late 2001.

Another prominent example of a bacterial spore former of concern is *Clostridium botulinum*. The bacterium and the spore are widespread in nature; for example, they are a common inhabitant of the soil. This bacterium can also survive in canned foods for extended time periods, even when the food has been heated or is acidic. When the food is eaten, the dormant bacteria begin to grow again and produce a variety of potent toxins that disrupt the nervous system, causing serious illness.

The contamination of foods by terrorists is a significant security concern, especially in the United States. Because the spores are hardy and can be transported virtually undetected, they could be taken to food plants or supermarkets, where the food could be contaminated. The spores would survive to cause illness.

Other microorganisms of human concern that form spores include protozoa (e.g., *Microsporidia*) and fungi (e.g., *Actinomycetes).*

Formation of bacterial spores. The multistep process of forming a spore is known as sporulation. The process begins when a bacterium senses that the environmental conditions are becoming life threatening. Bacteria are equipped with a whole battery of sensing proteins and other compounds that monitor environmental conditions of temperature, pH of the surrounding fluid, water content, and availability of food, as some examples. After monitoring the environment for a period of time, the deteriorating conditions trigger the microbe to begin the change from a growing and dividing cell to a dormant spore.

The genetic material of the bacterium is duplicated. Then, the membrane coat that surrounds the inside of the bacterium pinches inward until the ends of the inward growing membrane meet. This isolates one of the copies of the genetic material from the remainder of the bacterium. This smaller cell is called a daughter cell. The remainder of the bacterium is called the mother cell.

In the next stage of spore formation, the membrane that surrounds the mother cell surrounds the daughter cell. This creates a daughter cell that is surrounded by two layers of membrane. Between these two membranes a think layer of a rigid material forms. This layer is called peptidoglycan. Peptidoglycan is normally present in the bacterial cell wall, but not in nearly the same amount. The thick peptidoglycan makes the double membrane layer very tough and hard to break apart. Finally, this tough membrane is coated on the outer surface by proteins. The proteins are also resistant to breakage.

The remnants of the mother cell dissolve away leaving the spore. The spore is essentially in hibernation. There is very little chemical activity. Nevertheless, the spore is able to monitor the external environment and, when conditions are sensed as being more favorable, the conversion from the spore form to the growing organism begins.

The threat from spores. The threat from spores, particularly anthrax spores, lies in their small size and powdery texture once they have been dried. As shown in the anthrax attacks in the United States in 2001, anthrax spores can be delivered to someone in a letter. The spores escape detection using methods like an x ray. When the letter is opened, the spores can be dispersed in the air and breathed in.

Studies in animal models have shown that even the inhalation of a few spores is enough to cause an infection. The lung is an ideal environment for the anthrax bacterium. Food is available and the atmosphere is warm and moist. When the spores germinate into growing bacteria, the resulting infection can feel similar to the flu at first. Thus, a victim may not seek treatment, believing that the illness will pass in a few days. By the time the true nature of the infection is discovered, the infection can be so advanced as to be fatal.

Anthrax spores could also potentially be dispersed from an airplane or a balloon. Indeed, the terrorists responsible for the September 11, 2001 attacks on the World Trade Center and the Pentagon had explored the use of crop dusting aircraft. Models developed by the U.S. government have predicted that a few hundred pounds of anthrax spores released upwind of Washington, D.C. could cause at least several hundred thousand deaths within a few days.

The growing of the amounts of bacteria necessary to prepare large amounts of powdered spores and the preparation of the spores is not an easy task. Nonetheless, many microbiologists are capable of the task, and the construction of a facility that is large enough to house the needed equipment is not overly difficult. In the past century, nations including the U.S. and Russia had active anthrax weaponization programs. Prior to Operation Iraqi Freedom, Iraq was suspected of having an anthrax weapons development program.

Protection from spores. The threat posed by the use of spores in the mail is difficult to counter. Researchers are working to develop sensors that detect the spores, based on the reaction of antibodies with target proteins on the surface of the spores. However, such detection requires

physical contact with the spores. Methods that do not require the opening of letters, such as irradiation, are being tested and refined in the field and in the laboratory.

Another tact is the use of compounds that can destroy the spore. For example, in 2002, researchers discovered that an enzyme called PlyG lysin will chemically crack apart the spore coat. The spore contents are released and disintegrate. Until such sophisticated detection and protection methods are perfected, the treatment of a site contaminated with spores will continue to include the use of bleach.

FURTHER READING:

BOOKS:

Fischetti, Vincent, Richard P. Novick, Joseph J. Ferretti, and Danile A. Portnoy. *Gram-Positive Pathogens.* Washington: American Society for Microbiology Press, 2000.

Storz, Gisela, and Regine Hengge-Aronis. *Bacterial Stress Responses.* Washington: American Society for Microbiology Press, 2000.

Caipo, M.L., S. Duffy, L. Zhao, et al."*Bacillus megaterium* Spore Germination is Influenced by Inoculum Size." *Journal of Applied Microbiology.* no. 92 (2002): 879–84.

ELECTRONIC:

American Society for Microbiology. "Microbial Spore Formation." Microbe.org. 1999. <http://www.microbe.org/microbes/spores.asp>(10 January 2003).

SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Anthrax Weaponization
Biological Warfare
Food Supply, Counter-Terrorism
Mail Sanitization
Pathogens
Weapons of Mass Destruction, Detection

SR-71 Blackbird

CARYN E. NEUMANN

The SR-71, a black, high-altitude airborne reconnaissance platform that flew at trisonic speed, gave the United States the ability to photograph military sites in hostile countries as well as the opportunity to confirm interpretations of satellite photographs from 1968 until 1990. Photographs taken from SR-71s helped end the siege of Khe Sanh in Vietnam in 1968, preserved the Strategic Arms Limitation Treaty (SALT) with the Soviet Union by monitoring troop movements in Cuba in 1979, and confirmed that Iran had acquired Silk Worm missiles from China for possible use against oil tankers in the Straits of Hormuz in 1987. While of obvious military value, each SR-71 burned enormous amounts of fuel, and required a large amount of staff support. For reasons of economy, the Department of Defense terminated the program and the last SR-71 flew in 1990.

The SR-71, planned in the early 1960s as a weapon in the Cold War, gave the U.S. the ability to survey more than 100,000 square miles of Earth's surface in an hour's time. The 29 aircraft in service flew above 80,000 feet, higher than any other platform, and traveled at Mach 3.17–3.30 covering 30 miles every minute. The SR-71 could survey up to a quarter of a million square miles of territory in one sortie. High-strength lightweight titanium alloy covered 90% of the aircraft with 20% of the skin consisting of radar-transparent plastic. For missions, the platforms were fitted with either a high-resolution horizon-to-horizon optical bar camera or a radar package which generated film of the ground in all weather conditions. The SR-71 contained no armament.

The first operational flight of the SR-71 took place on March 21, 1968, and brought information crucial to the American war effort in Vietnam. Photos taken by the crew revealed the location of heavy artillery emplacements around Khe Sanh, an American garrison in Vietnam under siege by the North Vietnamese. By providing data that had previously eluded sensors on other aircraft, the SR-71 allowed the American command to direct B-52 bombers to the enemy site and helped to end an event which had riveted the attention of the public. In 1979, when a satellite revealed a large Soviet force in Cuba, an SR-71 flew continuing surveillance over the island to monitor the situation and ensure Senate ratification of SALT. A 1987 mission to Iran gathered extensive information about masses of military equipment in the Persian Gulf, including the presence of Silk Worms, land-based anti-ship missiles from China that the Iranians apparently intended to use to threaten merchant tankers in the Straits of Hormuz. The U.S. Navy received warning of the missiles and diplomats brought pressure on Iran to remove them. On 80 occasions in the 1980s when satellites broke down or were unable to see through the atmosphere, SR-71s provided reconnaissance imagery of vital areas in the Middle East.

The SR-71 penetrated hostile territory with comparatively little vulnerability to attack unlike other reconnaissance platforms like the U-2 spy plane. The workhorse U-2, however, operated for considerably less money and generally received reconnaissance assignments while the SR-71s remained in their hangars. The Department of Defense made the decision to terminate the program on November 22, 1989. Secretary of Defense Richard Cheney in June 1990 ordered that three SR-71 aircraft be placed into long-term storage for possible use in a future conflict. The SR-71s did not see service in the Gulf War, however, and most of their aircrews and skilled maintenance force

SR-71 Blackbird. ©GEORGE HALL/CORBIS.

are now unavailable because of the passage of time. As satellite technology involves less human risk and grows and more precise and cost-effective, it is uncertain that the United States will justify the cost of deploying SR-71 intelligence-gathering machines in the future.

FURTHER READING:

BOOKS:

Crickmore, Paul F. *Lockheed SR-71: The Secret Missions Exposed.* London: Osprey, 1988.

Thornborough, Anthony M. *Sky Spies: Three Decades of Airborne Reconnaissance.* London: Arms and Armour Press, 1993.

SEE ALSO

Photographic Resolution
Photography, High-Altitude
Satellites, Spy

Star Wars.

SEE *Strategic Defense Initiative and National Missile Defense.*

START I Treaty

ADRIENNE WILMOTH LERNER

The Strategic Arms Reduction Treaty, now known as START I, was one of the key weapons agreements forged during the détente period of the late Cold War era. Negotiations for strategic weapon reductions of the United States and Soviet Union arsenals began in 1982, when both nations sought a lessening of Cold War tensions. The initial enthusiasm for the treaty waned when the Soviet Union withdrew from talks regarding weapons reduction after the United States deployed several immediate-range missiles in allied nations in western Europe. Negotiations did not begin again until 1985, and then progressed slowly until the fall the Iron Curtain and Soviet-influenced communism in Eastern Europe. START I was finally signed by United States President George H. W. Bush and Soviet Premier Mikhel Gorbachev in Moscow on July 31, 1991.

START I called for a drastic reduction of United States and Soviet arsenals. The treaty was originally designed to cover a fifteen-year period, in which the total Cold War build-up of weapons would be reduced to a third of its pre-treaty strength. The two nations agreed to limit strategic

arms, and maintain similarly strengthened arsenals. The treaty covered not only warheads, but also long-range delivery vehicles including Intercontinental Ballistic Missiles (ICBMs). START I limited each nation to 1,600 nuclear delivery vehicles, 6,000 warheads, and less than 7,000 ballistic missile warheads. Both nations began developing plans and facilities for weapons destruction during the negotiation process, however, the United States was better equipped to handle limited disarmament at the time START I was signed.

Though an indication of diminishing Cold War era tensions between the two nations, the treaty was controversial. Some argued that the treaty handicapped new weapons development and downplayed national security threats from other nations aside from the Soviet Union. Environmentalists feared that large-scale weapons destruction would not be adequately planned or contained, causing damage similar to that of already controversial weapons testing.

The largest hurdle to START I, however, came just a few months after its ratification. In 1991, The Soviet Union dissolved, leaving its nuclear arsenal scattered in the newly independent nations of Russia, Ukraine, Kazakhstan, and Belarus. The four Soviet successor states signed an addendum to the START I treaty on May 23, 1992. The Lisbon Protocol to the START I treaty added these nations to the treaty, each agreeing to dismantle their weapons arsenals to meet the provisions of the original treaty. The protocol further bound the nations to a Nuclear Nonproliferation Treaty, strictly curtailing the sale or transmission of nuclear technology to non-nuclear nations and eliminating Soviet-era nuclear weapons from Soviet successor states, with the exception of Russia. Under the Cooperative Threat Reduction (CTR) program, all warheads in Ukraine, Belarus, and Kazakhstan were transferred back to Russia by 1997.

START I does not expire until 2009, but in December 2001, all START I reductions were completed. Russia and the United States signed a subsequent START treaty in 1993, and the Strategic Offensive Reductions Treaty (SORT) in 2002. These treaties further reduce the permitted number of strategic arms, but also address the problems of aging nuclear arsenals and the possibility of long-term weapons storage as an alternative to destruction.

■ FURTHER READING:

ELECTRONIC:

United States Department of Energy, *Atomic Century* <http://www.dpi.anl.gov/dpi2/hist_docs/treaties/start2.htm.> (20 December 2002).

SEE ALSO

START II

An SS-19 strategic missile warhead is loaded into a silo at a site near Saratov, Russia, in 1999. After languishung in the Russian parliament for almost seven years, the START II arms control treaty was finally ratified by Russia in 2000. AP/WIDE WORLD PHOTOS.

START II

■ ADRIENNE WILMOTH LERNER

START II, or the Further Reduction and Limitation of Strategic Offensive Arms Treaty, was drafted as an expansion of the 1991 Strategic Arms Reduction Treaty (START I). The treaties between Russia and the United States prescribed the reduction of national nuclear warheads, delivery systems, and ballistic missiles. START II proposed to reduce the arsenals of the United States and Russia to a third of their pre-treaty strength.

The second strategic arms reduction treaty was signed in Moscow on January 3, 1993. The treaty was not ratified by the U.S. Senate until three years later. In March 1997, at the Helsinki Summit, an addendum known as the Helsinki Protocol was added to START II and later ratified by both nations. The Helsinki Protocol allowed for an extended amount of time to achieve treaty objectives, giving both nations time to implement new programs for deactivation, storage, and destruction.

START II, with the Helsinki Protocol addendum, called for two phases of reduction. The first phase included a sizable reduction of warheads and demanded the complete deactivation of nuclear warhead delivery systems banned by the treaty by the end of 2004. The second phase proposed a further reduction of warheads and the destruction of deactivated missiles and delivery systems by December 31, 2007.

START II especially addressed post-Cold War relations between Russia and the United States, seeking to reduce the Cold War era build up of arms and forge new Russian-American cooperative strategies in regard to international nuclear policy. The treaty called for both nations to reduce their arsenals to approximately 3, 500 warheads. In addition to prescribing further deactivation of warheads, START II expanded limitations on delivery systems such as submarines, bombers, and ballistic missiles. A main American objective of START II negotiations was a ban on all Russian SS-18 missiles. The final treaty banned all current Multiple Independently Targetable Reentry Vehicles (MIRVs) missiles, or heavy ballistic missiles with multiple warheads, in both nations' deployed forces. This provision was mainly targeted at encouraging strategic disarmament in former Soviet satellite nations in Europe and Asia, and the dismantling of Russian and American "first strike capability" weapons.

START II prescribed the same rigid guidelines for weapons counting and destruction as START I. It further utilized the same policing, reporting, and confirmation committees as established by the former treaty.

START II was once again brought into the spotlight in 2002. Earlier moves by the U.S. government to amend, or even dissolve, a separate treaty with Russia regarding ballistic missiles, to allow possible construction of a missile defense system, prompted Russia to reevaluate their interest in continuing with START II arms reductions. In May 2002, U.S. President George W. Bush and Russian President Vladimir Putin signed a new weapons management treaty, the Strategic Offensive Reductions Treaty (SORT).

■ FURTHER READING:

ELECTRONIC:

United States Department of Energy, *Atomic Century* <http://www.dpi.anl.gov/dpi2/hist_docs/treaties/start2.htm.> (20 December 2002).

STASI

The *Ministerium für Staatssicherheit*, Ministry of State Security, was the primary intelligence and security agency of the German Democratic Republic (GDR), or East Germany, during the Cold War. The Stasi, as the organization was most commonly known, maintained a comprehensive network of informants, agents, and military-trained secret police. Stasi operations focused on political security and espionage, both domestically and abroad, aiding the Soviet KGB more than any other satellite intelligence organization. During its 39-year tenure, at least one-third of the population of East Germany was victimized by Stasi surveillance, arrest, detention, or torture.

The East German government, with the assistance of the Soviet intelligence community, established the Stasi on February 8, 1950. The organization's main charge was preserving the communist regime in East Germany through clandestine operations. The first Stasi agents were trained by the Soviet KGB. From the outset, the Stasi operated above the law. The agency's policies and operations were reviewed only by the Communist Central Committees in East Germany and the Soviet Union; in turn, the agency expressly served the political desires of the communist regime.

The Stasi created a widespread network of civilian informants. These informants were citizens who cooperated with Stasi agents, sometimes in exchange for money or goods. These unofficial informants used their jobs, social influence, and family networks to spy on fellow citizens. Informants were required to report suspicious or anti-government behavior to Stasi authorities. Tips from informants were followed by further agent surveillance or immediate arrest. The Stasi maintained its own network of detention camps and prisons, the most notorious of which was Bauden II. The Stasi garnered a reputation for its use of brutality, torture, and blackmail as routine methods of extracting information and coercing cooperation.

While the threat of Stasi non-member informants was great, the actual agent network of the Stasi was itself comprehensive. The agency used human intelligence to infiltrate factories, schools, and social and political organizations. Stasi officials created vast files on individuals that included photographs, surveillance reports, and even physical samples of hair or clothing. Stasi agents used scent samples, often bits of clothing sealed in airtight containers for storage, to track defectors or known dissidents using dogs.

The Agency itself was divided into several operational divisions, each focusing on various internal security tasks. The Ministry for State Security maintained one armed force, the *Feliks Dzierzynski* Guard Regiment (FD), named for the founder of the Bolshevik secret police. The force consisted of as many as 8,000 military-trained members. The FD guarded government and communist party personnel, government buildings, Soviet monuments, and military instillations. The FD employed special commando and intelligence units to conduct clandestine operations.

The Main Administration for Reconnaissance focused its espionage on foreign intelligence, most especially the nations of the North Atlantic Treaty Organizations (NATO)

Workers shown in this 1998 photo reconstituting the Stasi archives which were torn up and put into 17,000 bags. ©BOSSU REGIS/CORBIS SYGMA.

and neighboring West Germany. The division coordinated its intelligence findings with the Soviet KGB via the Main Coordinating Administration.

East Germany was a highly controlled censorship state. The Main Department for Communications Security operated an internal communications network fro the East German government and between East German and Soviet authorities. The department also culled government information from public media, and conducted counterespionage measures to secure lines against tapping devices. Surveillance of foreign diplomats, foreign residents, and occasional travelers was conducted by the Main Administration for the Struggle Against Suspicious Persons. Like East German citizens, foreigners in East Germany were subject to strict censorship and Stasi arrest.

Immediately before the fall of East Germany in 1989, the Stasi employed 91,000 staff members. Their active informer network included nearly 200,000 people. After the reunification of Germany on October 3, 1990, the German intelligence community was radically reorganized. In an attempt to restore public trust in the government in the former GDR, German officials banned employment in the new government of anyone who had worked for the East German Stasi. The extensive Stasi archives were opened to the public in 1991, permitting victims of Stasi surveillance to find out the names of agents and informers who had spied on them.

FURTHER READING:

BOOKS:

Koehler, John O. *STASI: The Untold Story of the East German Secret Police.* Boulder, CO: Westview Press, 1999.

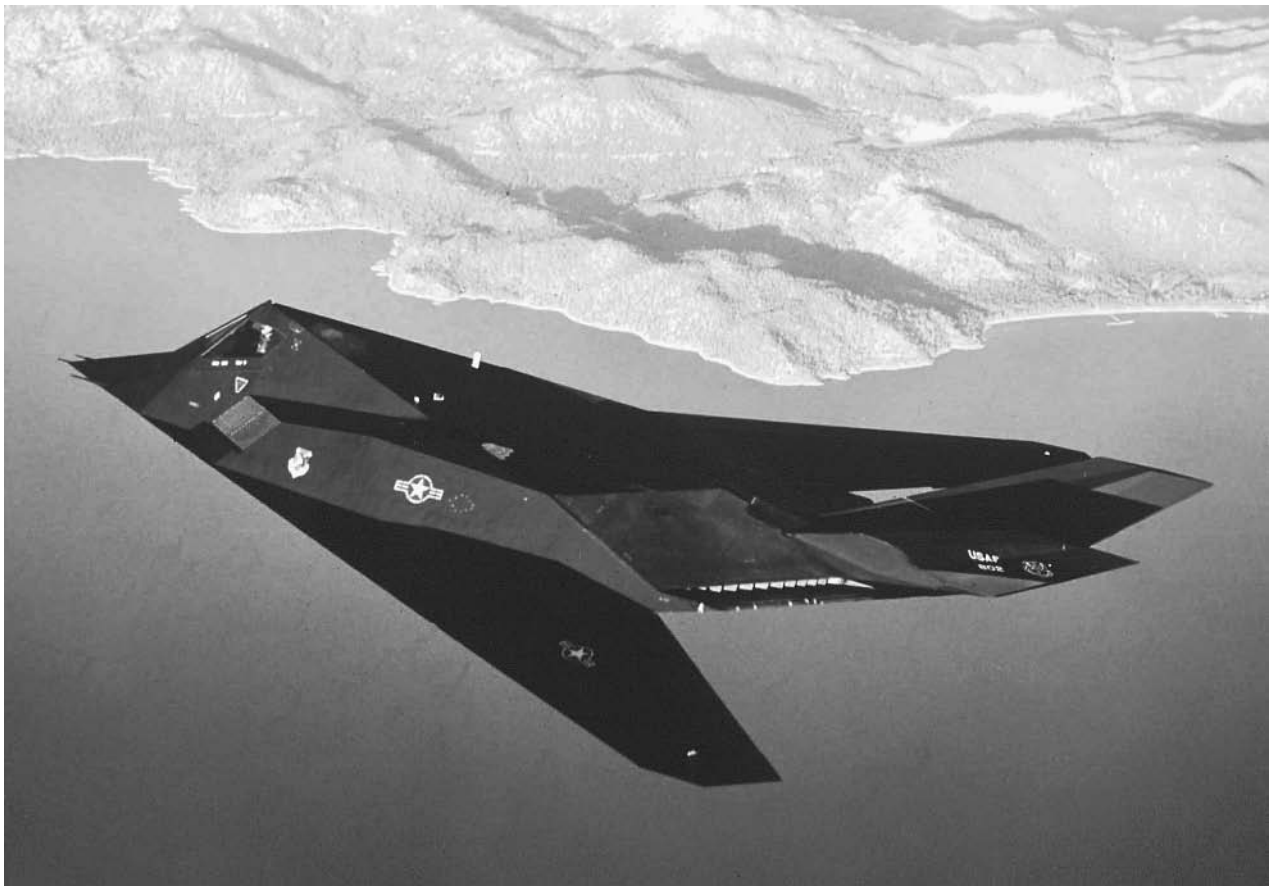
SEE ALSO

Berlin Tunnel
Berlin Wall
Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Germany, Intelligence and Security
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*

Stealth Technology

LARRY GILMAN

Stealth technology, also termed "low-observable" technology, is a set of techniques that render military vehicles, mostly aircraft, hard to observe. Because RADAR—an acronym for *RA*dio *D*etection *A*nd *R*anging—is the



An Air Force F-117 stealth fighter is shown in this undated Department of Defense photo. AP/WIDE WORLD PHOTOS.

primary detection technology for aircraft, most stealth technologies are directed at suppressing RADAR returns from aircraft, but stealth technology minimizes other "observables" as well, including energy emissions that of any kind that might be observed by an opponent. Stealth technology is deployed today on several types of aircraft and a few surface ships. Counter-stealth technologies are also under continuous development.

History of Stealth Technology

Development of stealth technology for aircraft began before World War I. Because RADAR had not been invented, visibility was the sole concern, and the goal was to create aircraft that were hard to see. In 1912, German designers produced a largely transparent monoplane; its wings and fuselage were covered by a transparent material derived from cellulose, the basis of movie film, rather than the opaque canvas standard in that era. Interior struts and other parts were painted with light colors to further reduce visibility. The plane was effectively invisible from the ground when flow at 900 ft (274 m) or higher, and faintly visible at lower altitudes. Several transparent German aircraft saw combat during World War I, and Soviet aircraft designers attempted the design of transparent aircraft in the 1930s.

With the invention of RADAR during World War II, stealth became both more needful and more feasible: more needful because RADAR was highly effective at detecting aircraft, and would soon be adapted to guiding antiaircraft missiles and gunnery at them, yet more feasible because to be RADAR-stealthy an aircraft did need to be not be completely transparent to radio waves; it could absorb or deflect them.

During World War II, Germany coated the snorkels of its submarines with RADAR-absorbent paint to make them less visible to RADARs carried by Allied antisubmarine aircraft. In 1945 the U.S. developed a RADAR-absorbent paint containing iron. It was capable of making an airplane less RADAR-reflective, but was heavy; several coats of the material, known as MX-410, could make an aircraft unwieldy or even too heavy to fly. However, stealth development continued throughout the postwar years. In the mid 1960s, the U.S. built a high-altitude reconnaissance aircraft, the Lockheed SR-71 Blackbird, that was extremely RADAR-stealthy for its day. The SR-71 included a number of stealth features, including special RADAR-absorbing structures along the edges of wings and tailfins, a cross-sectional design featuring few vertical surfaces that could reflect RADAR directly back toward a transmitter, and a coating termed "iron ball" that could be electronically

manipulated to produce a variable, confusing RADAR reflection. The SR-71, flying at approximately 100,000 feet, was routinely able to penetrate Soviet airspace without being reliably tracked on RADAR.

Development of true stealth aircraft (i.e., those employing every available method to avoid detection by visible, RADAR, infrared, and acoustic means) continued, primarily in the U.S., throughout the 1960s and 1970s, and several stealth prototypes were flown in the early 1970s. Efforts to keep this research secret were successful; not until a press conference was held on August, 22, 1980, after expansion of the stealth program had given rise to numerous rumors and leaks, did the U.S. government officially admit the existence of stealth aircraft. Since then, much information about the two U.S. stealth combat aircraft, the B-2 bomber and the F-117 fighter (both discussed further below), has become publicly available.

Design for stealth requires the integration of many techniques and materials. The types of stealth that a maximally stealthy aircraft (or other vehicle) seeks to achieve can be categorized as visual, infrared, acoustic, and RADAR.

Visual stealth. Low visibility is desirable for all military aircraft and is essential for stealth aircraft. It is achieved by coloring the aircraft so that it tends to blend in with its environment. For instance, reconnaissance planes designed to operate at very high altitudes, where the sky is black, are painted black. (Black is also a low visibility color at night, at any altitude.) Conventional daytime fighter aircraft are painted a shade of blue known as "air-superiority blue-gray," to blend in with the sky. Stealth aircraft are flown at night for maximum visual stealth, and so are painted black or dark gray. Chameleon or "smart skin" technology that would enable an aircraft to change its appearance to mimic its background is being researched. Furthermore, glint (bright reflections from cockpit glass or other smooth surfaces) must be minimized for visual stealth; this is accomplished using special coatings.

Infrared stealth. Infrared radiation (i.e., electromagnetic waves in the .72–1000 micron range of the spectrum) are emitted by all matter above absolute zero; hot materials, such as engine exhaust gases or wing surfaces heated by friction with the air, emit more infrared radiation than cooler materials. Heat-seeking missiles and other weapons zero in on the infrared glow of hot aircraft parts. Infrared stealth, therefore, requires that aircraft parts and emissions, particularly those associated with engines, be kept as cool as possible. Embedding jet engines inside the fuselage or wings is one basic design step toward infrared stealth. Other measures include extra shielding of hot parts, mixing of cool air with hot exhausts before emission; splitting of the exhaust stream by passing it through parallel baffles so that it mixes with cooler air more quickly; directing of hot exhausts upward, away from ground observers; and the application of special coatings to hot spots to absorb and diffuse heat over larger areas. Active countermeasures against infrared detection and tracking can be combined with passive stealth measures; these include infrared jamming (i.e., mounting of flickering infrared radiators near engine exhausts to confuse the tracking circuits of heat-seeking missiles) and the launching of infrared decoy flares. Combat helicopters, which travel at low altitudes and at low speeds, are particularly vulnerable to heat-seeking weapons and have been equipped with infrared jamming devices for several decades.

Acoustic stealth. Although sound moves too slowly to be an effective locating signal for antiaircraft weapons, for low-altitude flying it is still best to be inaudible to ground observers. Several ultra-quiet, low-altitude reconnaissance aircraft, such as Lockheed's QT-2 and YO-3A, have been developed since the 1960s. Aircraft of this type are ultralight, run on small internal combustion engines quieted by silencer-suppressor mufflers, and are driven by large, often wooden propellers. They make about as much sound as gliders and have very low infrared emissions as well because of their low energy consumption. The U.S. F-117 stealth fighter, which is designed to fly at high speed at very low altitudes, also incorporates acoustic-stealth measures, including sound-absorbent linings inside its engine intake and exhaust cowlings.

RADAR stealth. RADAR is the use of reflected electromagnetic waves in the microwave part of the spectrum to detect targets or map landscapes. RADAR first illuminates the target, that is, transmits a radio pulse in its direction. If any of this energy is reflected by the target, some of it may be collected by a receiving antenna. By comparing the delay times for various echoes, information about the geometry of the target can be derived and, if necessary, formed into an image. RADAR stealth or invisibility requires that a craft absorb incident RADAR pulses, actively cancel them by emitting inverse waveforms, deflect them away from receiving antennas, or all of the above. Absorption and deflection, treated below, are the most important prerequisites of RADAR stealth.

Absorption. Metallic surfaces reflect RADAR; therefore, stealth aircraft parts must either be coated with RADAR-absorbing materials or made out of them to begin with. The latter is preferable because an aircraft whose parts are intrinsically RADAR-absorbing derives aerodynamic as well as stealth function from them, whereas a RADAR-absorbent coating is, aerodynamically speaking, dead weight. The F-117 stealth aircraft is built mostly out of a RADAR-absorbent material termed Fibaloy, which consists of glass fibers embedded in plastic, and of carbon fibers, which are used mostly for hot spots like leading wing-edges and panels covering the jet engines. Thanks to the use of such materials, the airframe of the F-117 (i.e., the plane minus its electronic gear, weapons, and engines) is only about 10% metal. Both the B-2 stealth

bomber and the F-117 reflect about as much RADAR as a hummingbird

Many RADAR-absorbent plastics, carbon-based materials, ceramics, and blends of these materials have been developed for use on stealth aircraft. Combining such materials with RADAR-absorbing surface geometry enhances stealth. For example, wing surfaces can be built on a metallic substrate that is shaped like a field of pyramids with the spaces between the pyramids filled by a RADAR-absorbent material. RADAR waves striking the surface zigzag inward between the pyramid walls, which increases absorption by lengthening signal path through the absorbent material. Another example of structural absorption is the placement of metal screens over the intake vents of jet engines. These screens—used, for example, on the F-117 stealth fighter—absorb RADAR waves exactly like the metal screens embedded in the doors of microwave ovens. It is important to prevent RADAR waves from entering jet intakes, which can act as resonant cavities (echo chambers) and so produce bright RADAR reflections.

The inherently high cost of RADAR-absorbent, airframe-worthy materials makes stealth aircraft expensive; each B-2 bomber costs approximately $2.2 billion, while each F-117 fighter costs approximately $45 million; the U.S. fields 21 B-2s and 54 F-117s. The Russian Academy of Sciences, however, according to a 1999 report by *Jane's Defense Weekly*, claims to have developed a low-budget RADAR-stealth technique, namely the cloaking of aircraft in ionized gas (plasma). Plasma absorbs radio waves, so it is theoretically possible to diminish the RADAR reflectivity of an otherwise non-stealthy aircraft by a factor of 100 or more by generating plasma at the nose and leading edges of an aircraft and allowing it flow backward over the fuselage and wings. The Russian system is supposedly lightweight (>220 lb [100 kg]) and retrofittable to existing aircraft, making it the stealth capability available at least cost to virtually any air force. A disadvantage of the plasma technique that it would probably make the aircraft glow in the visible part of the spectrum.

Deflection. Most RADARs are monostatic, that is, for reception they use either the same antenna as for sending or a separate receiving antenna colocated with the sending antenna; deflection therefore means reflecting RADAR pulses in any direction other than the one they came from. This in turn requires that stealth aircraft lack flat, vertical surfaces that could act as simple RADAR mirrors. RADAR can also be strongly reflected wherever three planar surfaces meet at a corner. Planes such as the B-52 bomber, which have many flat, vertical surfaces and RADAR-reflecting corners, are notorious for their RADAR-reflecting abilities; stealth aircraft, in contrast, tend to be highly angled and streamlined, presenting no flat surfaces at all to an observer that is not directly above or below them. The B-2 bomber, for example, is shaped like a boomerang.

A design dilemma for stealth aircraft is that they need not only to be invisible to RADAR but to *use* RADAR; inertial guidance, the Global Positioning System, and laser RADAR can all help aircraft navigate stealthily, but an aircraft needs conventional RADAR to track incoming missiles and hostile aircraft. Yet the transmission of RADAR pulses by a stealth aircraft wishing to avoid RADAR detection is self-contradictory. Furthermore, RADAR and radio antennas are inherently RADAR-reflecting.

At least two design solutions to this dilemma are available. One is to have moveable RADAR-absorbent covers over RADAR antennas that slip aside only when the RADAR must be used. The antenna is then vulnerable to detection only intermittently. Even short-term RADAR exposure is, however, dangerous; the only stealth aircraft known to be have been shot down in combat, an F-117 lost over Kosovo in 1999, is thought to have been tracked by RADAR during a brief interval while its bomb-bay doors were open. The disadvantage of sliding mechanical covers is that they may stick or otherwise malfunction, and must remain open for periods of time that are long by electronic standards. A better solution, presently being developed, is the plasma stealth antenna. A plasma stealth antenna is composed of parallel tubes made of glass, plastic, or ceramic that are filled with gas, much like fluorescent light bulbs. When each tube is energized, the gas in it becomes ionized, and can conduct current just like a metal wire. A number of such energized tubes in a flat, parallel array, wired for individual control (a "phased array"), can be used to send and receive RADAR signals across a wide range of angles without being physically rotated. When the tubes are not energized, they are transparent to RADAR, which can be absorbed by an appropriate backing. One advantage of such an array is that it can turn on and off very rapidly, and only act as a RADAR reflector during the electronically brief intervals when it is energized.

Stealthy Flying

Stealth technology is most effective when combined with other measures for avoiding detection. For example, the F-117 and B-2 are both designed to fly at night, the most obvious visual stealth measure. Further, the F-117 is designed to fly close to the ground (i.e., at less than 500 feet [152 m]). Normal ground-based RADAR cannot see oncoming targets until they are in a line of direct sight, which, for a fast, low-flying aircraft approaching through hilly terrain, may not occur until the aircraft is almost above the RADAR. Even down-looking RADARs carried on aircraft have more difficulty tracking craft that are flying near ground-level, mingling their reflections with the noisy pattern of echoes from the ground itself ("ground clutter"). The F-117 therefore can fly close to the ground, swerving under computer control to avoid obstacles such as hills or towers. This flight style is known as jinking, snaking, or terrain following. (An aircraft such as the B-2 is too large to perform the rapid maneuvers required for jinking, and so flies at higher altitudes.)

At the opposite extreme from jinking flight, ultra-high altitudes have also been used for stealth purposes. Reconnaissance aircraft deployed by the U.S. since the 1950s, including the U-2 and the SR-71, have set most of the altitude records for "air-breathing" craft (i.e., craft that do not, like rockets, carry their own oxygen). Such planes fly near the absolute limit of aerodynamic action; if they went any higher, there would be not be enough air to provide lift.

Counter-stealth. An aircraft cannot be made truly invisible. For example, no matter how cool the exhaust vents of an aircraft are kept, the same amount of heat is always liberated by burning a given amount of fuel, and this heat must be left behind the aircraft as a trail of warm air. Infrared-detecting devices might be devised that could image this heat trail as it formed, tracking a stealth aircraft.

Furthermore, every jet aircraft leaves swirls of air—vortices—in its wake. Doppler RADAR, which can image wind velocities, might pinpoint such disturbances if it could be made sufficiently high-resolution.

Other anti-stealth techniques could include the detection of aircraft-caused disturbances in the Earth's magnetic field (magnetic anomaly detection), networks of low-frequency radio links to detect stealth aircraft by interruptions in transmission, the use of specially shaped RADAR pulses that resist absorption, and netted RADAR. Netted RADAR is the use of more than one receiver, and possibly more than one transmitter, in a network. Since stealth aircraft rely partly on deflecting RADAR pulses, receivers located off the line of pulse transmission might be able to detected deflected echoes. By illuminating a target area using multiple transmitters and linking multiple receivers into a coordinated network, it should be possible to greatly increase one's chances of detecting a stealthy target. No single receiver may record a strong or steady echo from any single transmitter, but the network as a whole might collect enough information to track a stealth target.

Stealth in wartime. Stealthy jet aircraft have been used for surveillance since the 1950s, but dedicated-design stealth warplanes were not used in combat prior to the first Gulf War (1991). In that war, F-117s—which first became operational in 1982—made some 1,300 sorties and were the only aircraft to bomb targets in downtown Baghdad. B-2 bombers were first used in combat in the Kosovo conflict in 1999, flying bombing sorties from Missouri to Yugoslavia (with midflight refueling over the Atlantic). F-117s were also used in the Kosovo conflict; one was shot down and two were damaged by enemy fire. The first overseas combat deployment of B-2 bombers occurred in 2003, during Operation Iraqi Freedom.

Stealth technology is also employed in U.S. cruise missiles such as the Tomahawk and the AGM-129A. The Tomahawk, a tactical weapon that can carry either nuclear or conventional warheads, has been deployed in four versions, including air-, sea-, and ground-launched types, and was used extensively in combat in both Gulf Wars and in Afghanistan in 2002. The AGM-129A is stealthier than the 1970s-vintage Tomahawk; it carries the W80 250-kiloton nuclear warhead and is designed to be fired from under the wings of the B-52H Stratofortress strategic bomber. The AGM-129A has not been used in combat.

FURTHER READING:

BOOKS:

Jones, Joseph. *Stealth Technology.* Blue Ridge Summit, PA: TAB Books, 1994.

PERIODICALS:

Hume, Andrew L., and Christopher Baker. "Netted RADAR Sensing," in Proceedings of the *CIE International Conference on RADAR, (IEEE)* 110–14, 2001.

ELECTRONIC:

"Russians Offer Radical Stealth Device for Export." Jane's Defence Weekly. March 17, 1999. <http://www.aeronautics.ru/plasma04.htm> (March 20, 2003).

SEE ALSO

SR-71 Blackbird
U-2 Incident
U-2 Spy Plane

Steganography

LARRY GILMAN

Steganography (from the Greek for "covered writing") is the secret transmission of a message. It is distinct from encryption, because the goal of encryption is to make a message difficult to read while the goal of steganography is to make a message altogether invisible. A steganographic message may also be an encrypted as an extra barrier to interception, but need not be. Steganography has the advantage that even a talented code-cracker cannot decipher a message without knowing it is there.

Steganography has been used since ancient times; Greek historian Herodotus records how one plotter of a revolt communicated secretly with another by shaving a slave's head, writing on his scalp, letting his hair grow back, and sending the slave as an apparently unencumbered messenger. The number of ways in which a steganographic message might be sent is limited only by human ingenuity. A photograph of a large group of people, for example, might contain a Morse-code message in the expressions

of the people in the photograph (e.g., smiling for dot, blank for dash) or in the directions they are looking (e.g., slightly to the left for dot, straight at the camera for dash). Writing in invisible ink or miniaturizing a message, as on microfilm, are also forms of steganography. Probably the commonest form of steganography involves the embedding of messages in apparently innocent texts, with the letters or words of the message indicated either by subtle graphic emphasis (e.g., heavier ink, lighter ink, a small defect) or by special positioning. For instance, reading the first word of every sentence in what appears to be an ordinary letter might yield a steganographic message.

Like most other forms of cryptography and secret writing, steganography has thrived in the digital era. Most digital documents contain useless or insignificant areas of data, or involve enough redundancy that some of their information can be altered without obvious effect. For instance, one might conceal a message bitstream inside a digital audio file by replacing the least-significant bit of every waveform sample (or every n^{th} waveform sample) with a message bit; the only effect on the file, if played back as audio, would be a slight decrease in the sound quality (probably imperceptible). Although steganographic messages can be hidden in any kind of digital files, image files, because they contain so much data to begin with, are usually used for digital steganography. Today a number of commercial or shareware programs exist for encoding text into steganographic images ("stego-images"), and are used by millions of people worldwide who wish to evade surveillance, especially by governments. This includes people who have reason to fear punishment for expressing their political ideas, as well as terrorists.

After the terrorist attacks of September 11, 2001, U.S. officials claimed that members of the group al-Qaeda, as well as of other terrorist groups, had used steganographic software to communicate plans to each other, hiding messages in images on pornographic Web sites and in sports chat rooms. Training camps for extremists in a number of countries now include instruction in cryptographic techniques, including digital steganography.

Steganography is also used for the less dramatic purpose of *watermarking*, which is the hiding of information indicating ownership or origin inside a digital file. (Physical watermarking, the practice after which digital watermarking is named, is the impression of a subtle pattern on paper using water. A watermark is only visible when the paper is held up to a light.) Watermarking can be used for digital authentication (i.e., to prove that certain party was indeed the source of a file) or to check whether a digital file was obtained in violation of copyright.

FURTHER READING:

BOOKS:

Kippenhahn, Rudolf. *Code Breaking: A History and Exploration.* Woodstock, NY: Overlook Press, 1999.

ELECTRONIC:

Johnson, Neil. "Steganography: Seeing the Unseen." IEEE Computer, February 7, 2001, 26–34. <http://www.jjtc.com/pub/r2026.pdf> (April 2, 2003).

Kelley, Jack. "Terror Groups Hide Behind Web Encryption." USA Today. February 5, 2001. <http:http://www.usatoday.com/tech/news/2001–02-05-binladen.htm> (April 2, 2003).

McCullagh, Declan. "Bin Laden: Steganography Master?" Wired News. February 7, 2001. <http://www.wired.com/news/politics/0,1283,41658,00.html> (April 2, 2003).

SEE ALSO

Cryptology, History

Strategic Defense Initiative and National Missile Defense

LARRY GILMAN

Since the advent of ballistic missiles at the end of World War II, the United States has considered several antiballistic missile (ABM) systems designed to defend against attack by intercontinental ballistic missiles (ICBMs) or, more recently, by shorter-range ballistic missiles. The Strategic Defense Initiative program and its successor, National Missile Defense (NMD), are the two most ambitious ABM schemes proposed to date. SDI sought, according to President Ronald Reagan's original vision (1983), a space-based ballistic-missile defense system that would render the United States safe from even an all-out Soviet attack involving thousands of missiles; NMD, evolved from SDI concepts in the post-Soviet environment, seeks effectiveness against launches of only one or a few missiles, possibly from "rogue states" such as North Korea. NMD thus returns to the limited design goals of the United States earliest ballistic-missile defense concepts of the 1960s.

Research on ABM systems began in the early 1950s. By the late 1960s, a nuclear-tipped interceptor missile dubbed Sentinel had been developed. Sentinel was designed to destroy incoming warheads by detonating near them, and was intended for deployment around major cities to protect them against accidental launch of one or several Soviet missiles or against a limited strike by China. The system was never deployed, however, and in 1969 President Richard Nixon announced that Sentinel would be renamed Safeguard and reassigned to protecting "our land-based retaliatory forces [i.e., nuclear-tipped ICBMs based in the American Midwest] against a direct attack by the Soviet Union." At this time, however, the United States and Soviet Union were nearing agreement that ballistic-missile defense (BMD) is inherently destabilizing.

U.S. President Ronald Reagan is flanked by physicist Dr. Edward Teller, left, and Lt. Gen. James A. Abrahamson, director of Strategic Defense Initiative, as he arrives to address a conference marking the first five years of his "Star Wars" missile defense program in 1988. AP/WIDE WORLD PHOTOS.

According to the standard anti-BMD argument, missile defenses encourage their possessor to start a nuclear war strategy because any BMD system will necessarily be more effective against a weakened counterattack than against a first strike; BMD therefore makes it "rational" to attack first. BMD proponents responded that missile defenses would enhance stability by adding to the uncertainties of a first strike. Nobody, during this period, argued that a perfect shield against nuclear attack was technically possible.

The Anti-Ballistic Missile Treaty of 1972 made the anti-BMD point of view official by forbidding the Soviet Union or United States to deploy extensive missile defenses. Each superpower was allowed by the original treaty to build ABM installations at two "widely separated" locations, each with at most 100 interceptor missiles. In 1974, a protocol was added to the ABM Treaty that reduced the number of permitted installations to one per nation. The United States chose to build its permitted ABM system near an ICBM base in Grand Forks, North Dakota; the Soviet Union deployed a system around Moscow. The Soviet system remains operational to this day, but the United States ABM system was shut down after only 9 months of operation in 1974–75 due to high operating costs and because strategists felt that the system was too small to make any strategic difference.

The ABM treaty's ban on significant defenses left deterrence through "mutually assured destruction" as an undisputed fact of life; that is, strategists hoped that neither superpower would dare start a nuclear war because annihilation of both societies would be the certain result. On March 23, 1983, however, President Reagan made a televised speech in which he declared that this situation was unacceptable. He asked, "Wouldn't it be better to save lives than to avenge them? . . . What if free people could live secure in the knowledge that their security did not rest upon the threat of instant U.S. retaliation to deter a Soviet attack, that we could intercept and destroy strategic ballistic missiles before they reached our soil or that of our allies?" This policy—far more ambitious than any ABM concept that had been contemplated before—was formalized by Reagan in National Security Decision Directive 85 two days later. Studies of the feasibility of an SDI-type system were made in the coming months, and a Strategic Defense Initiative Organization (SDIO) was chartered by Secretary of Defense Caspar Weinberger in April 1984.

Reagan's original proposal was conceptual, not technically specific. In October 1985, the SDIO released a set of five "architecture" studies describing possible configurations for an SDI system. The favored architecture suggested seven defensive layers, including air-, land-, sea-, and space-based components to track and shoot down ballistic missiles during their boost, cruise, and descent phases of flight. The main emphasis was on space-based defenses. Hundreds of satellites were proposed for command, control, and communications; remote sensing; battle management; and actual shootdown of targets.

A few of SDI's many proposals for destroying enemy missiles during each phase of flight, along with some of the countermeasures proposed for each proposal, are described below. Countermeasures are emphasized because many scientists and engineers in government, academia, and industry argued in the 1980s that it would be relatively easy to defeat SDI's proposed defenses using countermeasures, so no SDI system could ever replace deterrence. Today's debate concerning the feasibility of a more limited NMD program revives many of the measure-countermeasure concepts that were discussed during the SDI debate.

Proposals for Boost-Phase Intercept

The SDIO and its critics were agreed that it would be essential to destroy many enemy missiles during boost phase, the period during which a ballistic missile is being

accelerated by its rocket engines. With existing missile technology, boost phase lasts for 3 to 5 minutes. Boost-phase intercept is essential to defense against a large-scale ballistic missile attack because once the payload of a missile is no longer being accelerated, it can detach from its booster rocket and begin releasing independently targeted warheads (as many as 10 per missile) and hundreds of decoys (i.e., objects designed to confuse sensors). Once a large number of ballistic weapons achieve cruise phase, a "threat cloud" of hundreds of thousands of objects, mostly decoys, could be encountered. It would be impractical, for any defensive system of plausible size, to target every object in such a threat cloud during the few minutes available for cruise-phase defense; therefore, the size of the threat cloud has to be reduced by destroying missiles during boost phase. Some of the methods proposed for boost-phase intercept, along with countermeasures proposed for them, are discussed below.

Space-based directed-energy weapons. For boost-phase intercept the SDIO proposed several hundred satellites armed with powerful (i.e., >100 MW) lasers. Microwaves and neutral-particle beams (beams of hydrogen atoms) were also considered, but lasers were, and remain, the more developed technology. The directed-energy concept was, in essence, simple: lasers would cook boosters. Boosters contain flammable fuel and sensitive electronics and cannot carry armor because it would weigh too much, and so are more vulnerable to laser damage than, say, separated warheads, which are armored against the high heat of atmospheric reentry. Directed-energy weapons have two advantages for boost-phase intercept: First, they reach their targets in effectively zero time (at the speed of light or, in the case of a particle beam, at about half the speed of light). Second, after destroying one booster a directed-energy weapon can be retargeted, so each weapon can destroy a number of boosters. A basic limitation of any directed-energy weapon, however, is that it must illuminate or "dwell" on a booster for some period of time to destroy it. Dwell time for a laser of realistic power is generally estimated at between 1 second and 1 minute. Furthermore, redirection of the beam takes time, as it requires swiveling a mirror or other device. Finite dwell times and retargeting times, combined with the short duration of boost phase, place limits on the number of boosters that each directed-energy weapon can, in theory, destroy.

Space-based directed-energy weapons have the further limitation that beam intensity diminishes approximately with the square of the distance. They would therefore have to be placed in low (i.e., 120–3100 mi [200–5,000 km]) polar orbits, waiting to destroy boosting missiles not far below them. Low orbits, however, produce "absenteeism." That is, a low-orbit satellite can only see a small portion of the Earth at any one time, and so is absent from the sky over a particular area (e.g., Siberia) most of the time. To provide continuous coverage of a given area therefore requires many satellites. Absenteeism multiplies the number of weapon satellites needed to cover a specific launch zone by a factor of between 6 and 20; that is, for every satellite that happens to be passing over, say, Siberia at a given moment, at least six (or as many as 20) would have to be orbiting elsewhere, waiting their turn.

Surface-based directed-energy weapons. Two other SDI proposals for boost-phase intercept using directed-energy weapons were made. First was the use of fixed, ground-based optical lasers stationed in the continental United States. These lasers would send their beams up to orbital "fighting mirrors" which would reflect their energy back down over the horizon to enemy ballistic missiles in boost phase. The fighting mirrors would swivel rapidly to aim the laser light at the boosters. The lack of maneuverable mirrors that could reflect so much power without being destroyed by it was a major obstacle to this concept. Another technology, intensively urged by the SDIO for several years, was the nuclear-pumped x-ray laser. By surrounding a nuclear bomb with appropriate materials, it is possible in theory to cause those materials to lase (emit laser radiation, in this case in the x-ray part of the spectrum) briefly when the bomb explodes. If even a small fraction of the bomb's explosive energy is converted into x-ray laser energy, and this energy can be precisely aimed and focused, pulses powerful enough to destroy distant missiles could be generated. A basic limitation on this concept is that x rays cannot travel very far through the atmosphere; like space-based directed energy weapons (with the possible exception of optical-frequency lasers), nuclear-pumped x-ray lasers can only attack boosters during the portion of the boost phase that is above the densest part of the atmosphere, that is, above 50 to 56 miles (80–90 km). It was therefore proposed that nuclear-pumped x-ray lasers be deployed in a "pop-up" system. That is, they would be mounted on missiles deployed on land or at sea not far from the Soviet Union (or other potential enemy). When orbiting detectors observed the infrared signatures of ballistic missile launches (i.e., the infrared glow of hot rocket exhausts), the missiles bearing the nuclear-pumped x-ray laser devices would be launched within a few seconds (i.e., would "pop up"). They would race to the edge of space and there explode, destroying their targets before they could finish boost phase.

Proposals for Boost-Phase Countermeasures

Fast-burn boosters. As described above, boost-phase intercept must by definition gain access to target missiles during their boost phase, which lasts only 3 to 5 minutes. What is more, pop-up x-ray lasers and most proposed space-based directed-energy weapons can reach their targets only during that fraction of the boost phase which takes place in near-vacuum, because lasers and particle

beams tend to be scattered and absorbed by the atmosphere. Therefore, an important boost-phase countermeasure would be to build boosters that accelerate rapidly ("fast burn" boosters). With fast-burn boosters, boost phase would take place entirely within the atmosphere, reducing or eliminating the defense's chances for boost-phase interception using space-based or pop-up directed-energy weapons. Fast-burn boosters would in any case give boost-phase intercept less time to operate, which would require the defense to build more satellites, which could eventually become prohibitively expensive.

Booster hardening. Boosters could be coated with a material that ablates, or vaporizes, when illuminated by laser light. Such a coating could increase the dwell time needed to destroy a booster, again forcing the defense to build more satellites in order to cope with a given number of boosters in the time available.

Rotation. Boosters could be designed to spin as they fly. This would spread energy from an attacking laser over a larger surface area, increasing dwell time.

*Decoys.*Cheap rockets that simulate the infrared signature of real, weapons-carrying boosters could be deployed alongside real boosters. Such decoys could be made so numerous that no affordable defensive system could attack them all. Although decoy rockets might stagger and veer after launch, unlike real boosters, the real boosters might be deliberately programmed to stagger and veer like the cheap imitations, further confounding the defense. The later technique is termed "antisimulation": making a real weapon behave like a cheap decoy, rather than trying to make a cheap decoy that behaves like a real weapon.

Space mines. All space-based components of any SDI or NMD system would be vulnerable to space mines, which are simply bombs (possibly nuclear) orbiting near the defensive system's satellites. Before launching its ICBMs, the attacker would detonate its space mines. Since only one space mine is needed per battle station, and bombs are simpler than megawatt lasers, space mining would be intrinsically cheaper than defense building.

Kinetic weapons. Kinetic weapons (also termed "kinetic-kill weapons") destroy by virtue of their kinetic energy, that is, by colliding with their targets at high speed. Clouds of pellets orbited in the opposite direction to defensive satellites—released, probably, by space mines in appropriate orbits—could strike their targets at tens of thousands of miles per hour.

Directed-energy weapons. All the devices proposed for boost-phase intercept, including nuclear-pumped x-ray lasers, would be effective antisatellite weapons, and could therefore be used against an opponent's defensive satellites even more readily than they could be used against an opponent's missiles.

Nonballistic weapons. An enemy might employ weapons that do not have a boost phase at all. Cruise missiles (which fly at very low altitudes and can be made stealthy to both radar and infrared tracking), crewed aircraft, and bombs smuggled aboard ships or across land borders are all possible methods of making a nuclear attack that would not be vulnerable to boost-phase intercept.

Proposals for Cruise-Phase Intercept

SDI envisioned using the same orbital directed-energy stations described above for both boost-phase intercept and for cruise-phase intercept. However, SDI's designers anticipated that during cruise phase the task of distinguishing between actual warheads and the hundreds of thousands of radar reflectors, decoys, and other objects released after boost phase would become paramount. There would simply be too many objects to attack if one could not tell the warheads from the chaff and decoys. It was therefore proposed that "tapping" each object with a laser pulse and measuring its change in velocity might be used to determine which objects were heavy enough to be warheads; directed-energy weapons would then be used to destroy the real warheads.

Countermeasures for Cruise Phase

The primary cruise-phase countermeasure would be the release of large numbers of decoys. Atmospheric nuclear explosions could also be used to confuse or blind infrared sensors by providing a glowing background (as seen from space), and all methods mentioned above for destroying defensive satellites—orbital or ground-based directed-energy weapons, space mines, kinetic weapons, and so on—would also be threats to cruise-phase defense. Reactive decoy balloons that sensed a laser tap and accelerated themselves to mimic the mass of a real warhead were proposed as a countermeasure to "weighing" using laser pulses.

Proposals for Descent-Phase Intercept

Descent phase (also known as "terminal phase") is the period during which a warhead is falling through the atmosphere toward its target. Descent-phase intercept has the advantage that atmospheric friction will strip away all decoys released during cruise phase, sifting out the real warheads. Descent-phase intercept was the traditional, pre-SDI focus of ballistic-missile defense; the Sentinel system, for example, was designed to use high-altitude nuclear explosions to knock out enemy warheads in descent phase, and the primary focus of post-SDI ballistic-missile defense concepts has also been on descent-phase intercept. Since electromagnetic pulse (EMP) from high-altitude nuclear explosions could cripple communications and electrical systems over a continent-sized area, descent-phase intercept concepts since Sentinel have focused on kinetic-kill weapons that would actually strike their targets.

Countermeasures for Descent Phase

Possible countermeasures for descent phase are few, but stealth technology could make warheads harder to track; furthermore, the attacker is favored in descent phase by the great speed and small size (>1.5 m long, >.5 m wide at the base) of each cone-shaped warhead. To strike even a single incoming warhead moving at some 10,000 miles per hour, much less hundreds or thousands of them simultaneously, is an extremely difficult rocketry problem, often compared to hitting a bullet with a bullet in midair. Since the inception of the SDI program a number of tests have been conducted in which kinetic weapons (also termed "kinetic kill vehicles") have intercepted, or sought to intercept, incoming missiles or warhead-like objects, but most tests have failed or produced ambiguous results. Nevertheless, kinetic descent-phase intercept is not impossible, and continuing technological advances may render it more reliable.

The measures-countermeasures debate was vigorous during the 1980s because both sides agreed that a defensive system that allowed even 1% of the Soviet Union's 8,000 or so strategic warheads to reach the United States—80 thermonuclear weapons—could not protect United States society from destruction. The technical side of the SDI debate therefore revolved around the question of whether a BMD system providing better than 99% defensive coverage was buildable or not, and if so, whether it could be built within a plausible budget. In general, the countermeasures school prevailed. SDI funding was cut back in the late 1980s and the SDIO retreated from its original goal of "render[ing] nuclear weapons impotent and obsolete" (in President Reagan's 1983 words) to the traditional concept of defense against *limited* ballistic-missile attack. The SDIO was renamed the Ballistic-Missile Defense Organization (BMDO) in May, 1993, and its official emphasis was shifted away from space-based defenses, marking the end of the SDI period.

After SDI: GPALS and NMD

Three years before the term "strategic defense initiative" was abandoned, SDI officially gave up on being the total nuclear umbrella proposed by President Reagan in 1983. At the order of President George H. Bush, the program assumed in 1990 a more limited mission: Global Protection against Limited Strikes (GPALS). GPALS resembled Sentinel, in seeking to defend only against accidental or small-scale ballistic attacks, rather than massive launches of thousands of missiles. It differed from pre-SDI ballistic-missile defense in that it envisioned *global* protection, especially "theatre" defense against ballistic missiles fired in extended combat zones far from the continental United States.

During the 1990s, the term National Missile Defense (NMD) replaced GPALS, and the program re-evolved many features of SDI, albeit on a smaller scale. Today, NMD proposes a system with boost-phase, cruise-phase, and descent-phase intercept layers, much like SDI, only not intended to cope with the simultaneous launch of thousands of attacking missiles.

For boost-phase intercept NMD proposes lasers, both airborne and space-based. The airborne laser—already built and test-flown, and scheduled to attempt its first missile shoot-down test in 2003 or 2004—would be flown on a modified Boeing 747, use hydrogen fluoride lasing in the infrared part of the spectrum, have a range of several hundred kilometers, and be directed against theatre (short- and medium-range) ballistic missiles. Adaptive optics that measure atmospheric distortion between the weapon and the target would be an essential component of such a system. Having measured the atmospheric distortion in real time, the weapon imparts an inverse distortion to the laser beam as it fires; the predistortion and the actual atmospheric distortion cancel each other out, allowing a focused beam to dwell on the missile. (A similar technique is widely applied in ground-based astronomy.) NMD also proposes to eventually use space-based lasers for boost-phase intercept. The weapons proposed, a product of research begun under SDI, would consist of infrared (hydrogen fluoride) lasers in low orbits. However, the technical hurdles to such a system are numerous, even disregarding possible countermeasures, and funding for the space-based boost-intercept component of NMD has lately been reduced.

For both cruise and descent (midcourse and terminal) defense, NMD proposes to use kinetic-kill warheads that would destroy by collision. Both land-based and sea-launched kinetic-kill missiles are under development for these phases of defense.

NMD architecture. The detailed structure of the proposed NMD shift frequently, depending on technological and political factors. One typical, recently proposed NMD architecture consists of six essential elements:

1) A satellite system for the detection and tracking of missile launches, the first components to be launched in 2006 or 2007. The system consist of six geosynchronous satellites designed to observe the infrared emissions of booster rockets.

2) Approximately five ground-based early-warning radars to project the approximate trajectories of missiles detected by the infrared satellite system.

3) A number of high-frequency ground-based radars in the United States, United Kingdom, Greenland (Denmark), South Korea, and perhaps other locations, designed to discriminate between warheads and decoys during the cruise phase.

3) A midcourse (exoatmospheric) kinetic-kill interceptor missile, to be guided by information received from ground radars. The kinetic-kill warhead or vehicle is thrown

by its booster as nearly as possible toward its target, then guides itself during final approach using onboard sensors, computers, and steering rockets.

4) A "Battle Management, Command, Control, and Communications" network of ground stations where computers will integrate information from sensors, fire and guide interceptors, and assess success and failure in real time so that multiple attempts can be made on a given target if necessary.

The United States withdrew from the ABM Treaty in 2002, allowing it to begin construction on a preliminary cruise-phase kinetic-kill interceptor site in June 2002, in Fort Greely, Alaska. The 16-missile complex is scheduled for completion in 2004.

FURTHER READING:

BOOKS:

Causewell, Erin V. *National Missile Defense: Issues and Developments.* New York: Novinka Books, 2002.

Drell, Sidney D., Philip J. Farley, and David Holloway. *The Reagan Strategic Defense Initiative: A Technical, Political, and Arms Control Assessment.* Cambridge, MA: Ballinger Publishing Co., 1990.

PERIODICALS:

Bethe, Hans A., et al. "Space-Based Ballistic-Missile Defense." *Scientific American.* (October, 1984).

Fowler, Charles. "National Missile Defense (NMD)." *IEEE Aerospace and Electronic Systems Society (AESS) Systems Magazine* (January, 2002):4–12.

Lewis, George N., and Theodore A. Postol. "Future Challenges to Ballistic-Missile Defense." *IEEE Spectrum* (September, 1997): 6–68.

SEE ALSO

Ballistic Missiles
Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union

Strategic Petroleum Reserve, United States

WILLIAM J. ENGLE

The Strategic Petroleum Reserve (SPR), located in the United States and operated by the Department of Energy (DOE), is the largest emergency supply system of oil in the world. To enhance national security, in a Presidential Order signed November 13, 2001, President George W. Bush ordered the U.S. Department of Energy (DOE) to fill the Strategic Petroleum Reserve. The oil will come from royalty-in-kind transfers between the Department of the Interior and the DOE.

The SPR is designed to act as a "first line of defense" against a reduction of oil supplies to the United States. The president can release the stored oil as necessary—including a release to stabilize prices. In addition to the SPR, there are also a Naval Petroleum Reserve and special emergency reserves of home heating oil maintained in storages tanks (some rented from commercial sources in other areas of the country).

The Strategic Petroleum Reserve (SPR) contains a mixture of oil from domestic and foreign sources.

The SPR is presently made up of four underground storage facilities located in salt domes along the coastal regions of Louisiana and Texas and has a total storage capacity of 700 million barrels of oil. These sites were chosen from among the more than 400 potential areas along the Gulf Coast of the southern United States after careful review of their relative geologic characteristics.

A salt dome is a body of rock salt surrounded by layers of sedimentary rock. Geologic characteristics considered in selecting storage sites include: 1) area geologic activity, 2) structural size, 3) existence of a trapping mechanism, 4) salt geometry, 5) salt composition, and 6) surface conditions.

Geologic activity in the area of potential storage sites must be well understood. The coastal plains along the Gulf Coast tend to be in a perpetual state of either subsidence or uplift and the rate of such relative change must be measurable and predictable.

Structural size is a significant factor. Oil is stored in cylindrically shaped caverns constructed within the salt body that are typically 200 feet in diameter and approximately 2,000 feet in height or larger. A storage dome may consist of from one to more than twenty caverns in a three-dimensional pattern. Salt domes along the Gulf Coast typically range between being one half to five miles in diameter and may be over 20,000 feet in vertical height.

Fluid naturally flows through permeable strata just as water passes through a sponge. Oil will seek the highest possible level due to its relatively low specific gravity and would float to the surface if not otherwise trapped. A salt dome must be overlain by a trapping mechanism in order to be an environmentally safe and an economically secure storage site, Cap rock is a stratum of rock lacking permeability that can act as a trapping mechanism. However, not all salt domes are overlain by cap rock.

Salt domes are usually formed as the lighter salt rises through sedimentary strata above in a plastic state from a deeper source while forming irregular shaped and sometimes freestanding columns. The three dimensional geometry of the salt diapir must be profiled in order to facilitate the design of the storage cavern pattern.

Ideally the salt dome is composed of homogenous halite free of shale or other sedimentary rock. The presence of irregularities in composition may effect cavern construction and containment integrity.

Surface conditions play a role in site selection and project design, construction and ease of operation. Typically such sites are located in marsh areas or beneath standing water. Proximity to existing infrastructure supporting oil import, delivery and water handling is a major cost and operational consideration.

Though geologically complex, salt domes have proven to be a reliably safe and economically competitive means of storing oil for future use and play a key role in national energy management and supply.

FURTHER READING:

ELECTRONIC:

U.S. Department of Energy. "Fossil.Energy.gov Petroleum Reserves." <http://www.fe.doe.gov/program_reserves.html> (March 2, 2003).

SEE ALSO

DOE (United States Department of Energy) Petroleum Reserves, Determination

Stun Gun.

SEE *Less Lethal Weapons Technology.*

Sudan, Intelligence and Security

Due to its role with connection to the international war on terrorism, Sudan has much greater importance in the realm of intelligence and security than do most nations of Africa's interior. Though it harbored al-Qaeda leader Osama bin Laden from 1991 to 1996, Sudan in 2001 became an unlikely ally of the United States in its efforts against Islamist terrorists.

The two principal intelligence agencies of the Sudanese government are Al Amn al-Dakhili and Al Amn al-Khariji, the bureaus of internal and external security respectively. Security issues in Sudan have, for the most part, sprung from internal issues, particularly a civil war with roots going back to the 1950s. The vast nation, Africa's largest geographically, is sharply divided culturally into northern and southern regions. The north, which the government controls, is Arabic and Islamic, whereas the south is sub-Saharan African and non-Muslim (either Christian or traditionalist). The opposition Sudan People's Liberation Army (SPLA) controlled much of southern Sudan by the end of the twentieth century.

The Sudanese government has been notorious for its human rights violations, including the continuation of the black African slave trade in the 1990s. Its imposition of strict Muslim law on the south in 1983 sparked a civil war that claimed more than 1.5 million lives over the next 15 years. Meanwhile, the government in Khartoum provided safe haven to bin Laden, who had been exiled from his native Saudi Arabia. U.S. and Saudi pressure forced the Sudanese to eject bin Laden in 1996.

After the al-Qaeda attacks on U.S. embassies in Kenya and Tanzania in 1998, the U.S. military struck back at targets in Afghanistan and Sudan, whose Shifa Pharmaceutical Plant was reportedly making chemical weapons. In 2001, the *Financial Times* revealed that two months before the bombings, Sudanese external security bureau chief Gutbi al-Mahdi approached the regional head of the Federal Bureau of Investigation and offered to share intelligence on al-Qaeda. Suspicious of Khartoum, the administration of President William J. Clinton declined the offer.

The inauguration of President George W. Bush in 2001 signaled a change in U.S.-Sudanese relations. Even before the September 11 terrorist attacks, Sudanese intelligence had begun providing Washington with information on suspected terrorists who had resided in the country during the period 1991–96. Soon after the attacks, a senior State Department official told the *Washington Post* that Khartoum had made an "implicit" offer for the use of its military bases to strike against al-Qaeda. In March 2002, Sudanese authorities captured and imprisoned Anas Al-Liby, a senior al-Qaeda militant.

The Khartoum government made a peace deal with the SPLA in July 2002, and the two sides began work toward a ceasefire agreement.

FURTHER READING:

PERIODICALS:

"Accused Al Qaeda Senior Militant Captured in Sudan." *Los Angeles Times.* (March 17, 2002): A20.

Alden, Edward, and Mark Turner. "Sudan's Surprise Deal with Rebels Catches Washington Off-Guard." *Financial Times.* (July 23, 2002): 10.

Huband, Mark. "U.S. Rejected Sudanese Files on al-Qaeda." *Financial Times.* (November 30, 2001): 1.

ELECTRONIC:

Sipress, Alan. "Sudan Provides Administration Intelligence on Bin Laden." *Wall Street Journal* (September 30, 2001): A14.

Sudan: Intelligence Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/sudan/index.html> (March 1, 2003).

SEE ALSO

Egypt, Intelligence and Security
Kenya, Bombing of United States Embassy
Libya, Intelligence and Security

Suez Canal

As the longest canal in the world without locks, the Suez Canal links the Mediterranean and Red seas across the Isthmus of Suez. Although Eygpt's ancient rulers devised a means of connecting the Nile River to the Red Sea, it was only in modern times that French engineer Ferdinand de Lesseps developed a workable design for the 101-mile (163-km) canal, which opened in 1869. In 1956, the canal became the site of an international crisis involving Britain, France, Egypt, and Israel. Today the canal remains a strategic point of movement of the world's oil supply.

Early history. From ancient times, trade flourished in the Mediterranean and Red Seas, and pharaohs recognized the advantage to be gained by connecting the two bodies. As early as 1500 B.C., pharaohs of Egypt's New Kingdom commissioned the building of a canal between the Nile and the Red Sea. This early canal was covered by sand, and though the late seventh century B.C. pharaoh Necho II attempted to build a new canal, the project would not be completed until the Persian invasion of Darius after 522 B.C. This canal eventually met the same fate as its predecessors, and successive rulers—the Greeks under Ptolemy I and Cleopatra, and later the Romans under Trajan—attempted to restore it, but in each case the canal fell into disrepair.

Napoleon Bonaparte, when he conquered Egypt in 1798, revived the idea of a canal, this one to directly connect the two seas. The project did not begin for half a century, however, due to engineers' misconceptions regarding relative water levels. Finally, Lesseps, the former French consul to Egypt, received a 99-year concession on the canal from the khedive of Egypt. With a crew of some 2.4 million Egyptian workers, he commenced the building project, which cost more than 125,000 lives over the course of a decade. The canal opened with much ceremony on November 17, 1869.

Crisis and concerns. Until the Suez Crisis of 1956, the Anglo-French Suez Canal Company controlled the canal. Egyptian president Gamal Abdel Nasser had developed increasingly close ties with the Communist bloc, and therefore, when he requested assistance in building the Aswan High Dam—a project intended to tame the Nile and provide hydroelectric power to Egypt—the United States, Britain, and France refused. On July 26, Nasser retaliated by declaring martial law in the canal zone and seizing control of the canal.

Britain and France at first tried diplomacy, and when this failed, they sought Nasser's overthrow through an alliance with Israel. The three nations followed a classic "good cop/bad cop" strategy. On October 29, the Israelis invaded Egypt, whereupon Britain and France went into presented themselves as peacekeepers, and offered to occupy the canal zone on behalf of the United Nations (UN). Their actions raised such tensions among the two superpowers that both the United States and the Soviet Union very nearly intervened. The UN forced the evacuation of the French and British on December 22, and Israel pulled out in March 1957.

Aftermath of the Suez Crisis. The Suez Crisis raised the stature of Nasser immeasurably, and he has remained a powerful symbol to Arab nationalists such as Iraq's Saddam Hussein, the late Hafez al-Assad of Syria, and Libya's Muammar al-Qaddafi. The incident also marked the end of British and French influence in the Middle East, where they had held considerable sway for the better part of 150 years. From an intelligence standpoint, the Suez Crisis was significant for the role played by British interception of cipher transmissions, an operation known as Engulf.

Israel captured the Sinai Peninsula in the 1967 Arab-Israeli war, and for the next six years, the canal served as a buffer between Egypt and Israel. It was closed during that time, and the Egyptians, who regained control in 1973, only reopened it in 1975. Since then, they have widened it twice, and have plans to widen it again by 2010 so as to accommodate larger oil-carrying vessels. The U.S. Department of Energy has identified the Suez Canal as one of several geographic "chokepoints"—narrow passages that are both vital to the international oil trade and extremely susceptible to attacks or accidents.

FURTHER READING:

BOOKS:

Immermann, Richard H. *John Foster Dulles and the Diplomacy of the Cold War.* Princeton, NJ: Princeton University Press, 1990.

Kelly, Saul, and Anthony Gorst. *Whitehall and the Suez Crisis.* Portland, OR: Frank Cass, 2000.

Kunz, Diane B. *The Economic Diplomacy of the Suez Crisis.* Chapel Hill: University of North Carolina Press, 1991.

Kyle, Keith. *Suez.* New York: St. Martin's Press, 1991.

ELECTRONIC:

World Oil Transit Chokepoints. U.S. Department of Energy. <http://www.eia.doe.gov/emeu/cabs/choke.html> (April 1, 2003).

SEE ALSO

Egypt, Intelligence and Security

Engulf, Operation
Israel, Intelligence and Security
Middle East, Modern U.S. Security Policy and Interventions
United Kingdom, Intelligence and Security

Suitcase Bombs.

SEE *Russian Nuclear Materials, Security Issues.*

Supercomputers

BRIAN HOYLE

A supercomputer is a powerful computer that possesses the capacity to store and process far more information than is possible using a conventional personal computer.

An illustrative comparison can be made between the hard drive capacity of a personal computer and a supercomputer. Hard drive capacity is measured in terms of gigabytes. A gigabyte is one billion bytes. A byte is a unit of data that is eight binary digits (i.e., 0's and 1's) long; this is enough data to represent a number, letter, or a typographic symbol. Premium personal computers have a hard drive that is capable of storing on the order of 30 gigabytes of information. In contrast, a supercomputer has a capacity of 200 to 300 gigabytes or more.

Another useful comparison between supercomputers and personal computers is in the number of processors in each machine. A processor is the circuitry responsible for handling the instructions that drive a computer. Personal computers have a single processor. The largest supercomputers have thousands of processors.

This enormous computation power makes supercomputers capable of handling large amounts of data and processing information extremely quickly. For example, in April 2002, a Japanese supercomputer that contains 5,104 processors established a calculation speed record of 35,600 gigaflops (a gigaflop is one billion mathematical calculations per second). This exceeded the old record that was held by the ASCI White-Pacific supercomputer located at the Lawrence Livermore National Laboratory in Berkeley, California. The Livermore supercomputer, which is equipped with over 7,000 processors, achieves 7,226 gigaflops.

These speeds are a far cry from the first successful supercomputer, the Sage System CDC 6600, which was designed by Seymour Cray (founder of the Cray Corporation) in 1964. His computer had a speed of 9 megaflops, thousands of times slower than the present day versions. Still, at that time, the CDC 6600 was an impressive advance in computer technology.

Beginning around 1995, another approach to designing supercomputers appeared. In grid computing, thousands of individual computers are networked together, even via the Internet. The combined computational power can exceed that of the all-in-one supercomputer at far less cost. In the grid approach, a problem can be broken down into components, and the components can be parceled out to the various computers. As the component problems are solved, the solutions are pieced back together mathematically to generate the overall solution.

The phenomenally fast calculation speeds of the present day supercomputers essentially corresponds to "real time," meaning an event can be monitored or analyzed as it occurs. For example, a detailed weather map, which would take a personal computer several days to compile, can be complied on a supercomputer in just a few minutes.

Supercomputers like the Japanese version are built to model events such as climate change, global warming, and earthquake patterns. Increasingly, however, supercomputers are being used for security purposes such as the analysis of electronic transmissions (i.e., email, faxes, telephone calls) for codes. For example, a network of supercomputers and satellites that is called Echelon is used to monitor electronic communications in the United States, Canada, United Kingdom, Australia, and New Zealand. The stated purpose of Echelon is to combat terrorism and organized crime activities.

The next generation of supercomputers is under development. Three particularly promising technologies are being explored. The first of these is optical computing. Light is used instead of using electrons to carry information. Light moves much faster than an electron can, therefore the speed of transmission is greater.

The second technology is known as DNA computing. Here, recombining DNA in different sequences does calculations. The sequence(s) that are favored and persist represent the optimal solution. Solutions to problems can be deduced even before the problem has actually appeared.

The third technology is called quantum computing. Properties of atoms or nuclei, designated as quantum bits, or qubits, would be the computer's processor and memory. A quantum computer would be capable of doing a computation by working on many aspects of the problem at the same time, on many different numbers at once, then using these partial results to arrive at a single answer. For example, deciphering the correct code from a 400-digit number would take a supercomputer millions of years. However, a quantum computer that is about the size of a teacup could do the job in about a year.

FURTHER READING:

BOOKS:

Stork, David G. (ed) and Arthur C. Clarke. *HAL's Legacy: 2001's Computer Dream and Reality.* Boston: MIT Press, 1998.

ELECTRONIC:

Cray Corporation. "What Is a Supercomputer?" Supercomputing. 2002. <http://www.cray.com/supercomputing>(15 December 2002).

A technician monitors IBM's ASCI White in 2000, then the world's fastest supercomputer, that is capable of 12 trillion calculations per second. The Department of Energy uses ASCI White to analyze and protect the nation's nuclear weapons stockpile. AP/WIDE WORLD PHOTOS.

The History of Computing Foundation. "Introduction to Supercomputers." Supercomputers. October 13, 2002. <http://www.thocp.net/hardware/supercomputers.htm>(15 December 2002).

SEE ALSO

Computer Hardware Security
Information Warfare

Surgeon General and Nuclear, Biological, and Chemical Defense, United States Office

Among its many responsibilities, the Office of the United States Surgeon General serves as a clearinghouse for information on what is known as "medical NBC"—that is, the biomedical effects of nuclear, biological, and chemical (NBC) weapons and agents. Through the World Wide Web, the Surgeon General's office keeps physicians, as well as the general public, informed of dangers associated with anthrax, weapons of mass destruction, and other threats that became a part of public discourse after the terrorist attacks of September, 2001 and the subsequent war on terror.

The Office of the Surgeon General of the United States dates back to 1871, when President Ulysses S. Grant established the position. Appointed by the President with the advice and consent of the U.S. Senate, the Surgeon General serves a four-year term and reports to the Assistant Secretary for Health, principal advisor to the Secretary of Health and Human Services (HHS) on public health and scientific issues. The Surgeon General holds the rank of vice admiral in the U.S. Public Health Service Commissioned Corps, a uniformed service.

The Surgeon General Medical NBC Server was established after September 2001, to provide a reference and learning source on medical NBC matters. Although it is directed toward physicians, much of the information on the site (http://www.nbc-med.org) is accessible to citizens without medical training. The site was intended to supplement the Army Medical Department Center and School Distance Learning effort, and to coordinate with existing initiatives to provide Internet access to all medical facilities, both stationary and in the field. The Medical NBC Server also provides health advisories from groups that include the Food and Drug Administration, HHS, and even the U.S. Postal Service.

■ FURTHER READING:

ELECTRONIC:

Medical NBC Online Information Server. <http://www.nbc-med.org/> (April 2, 2003).

Office of the Surgeon General. <http://www.surgeon-general.gov/> (April 2, 2003).

SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Biological Warfare
Biological Warfare, Advanced Diagnostics
CDC (United States Centers for Disease Control and Prevention)
Public Health Service (PHS), United States
USAMRICD (United States Army Medical Research Institute of Chemical Defense)
USAMRIID (United States Army Medical Research Institute of Infectious Diseases
Weapons of Mass Destruction

Sweden, Intelligence and Security

Sweden established its national intelligence services in 1937, in response to escalating political and military tensions in Europe and the rise of Nazi Germany. While the Swedish military had maintained a unit of trained espionage and counterespionage agents since the early nineteenth century, the nation lacked a modern and specialized intelligence force. The initial intelligence services consisted of a central intelligence agency, a cryptology department, and a signals intelligence department.

Sweden's cryptology department, despite rudimentary equipment, quickly gained fame. In cooperation with the the signals intelligence department and the Navy, Swedish intelligence intercepted and deciphered nearly half of all German radio and wire transmissions in the years immediately preceding World War II. During the War, Nazi Germany considered Sweden's cryptology department on of its primary security threats. Sweden's intelligence services and cryptologists worked closely with some Allied forces, and in the eary war years, provided key information to British cryptologists at Bletchley Park.

After the war, Sweden's geographic location made it a useful station for monitoring Eastern Europe and the Soviet Union during the Cold War. Today, Sweden is a member of the European Union and contributes signals intelligence, as well as cryptological technology, to European cooperative intelligence operations. Though the country has a stated policy of neutrality, Sweden maintains one of Europe's largest and best-equipped intelligence forces.

The Swedish intelligence community does not use the traditional internal and external intelligence divisions within its various branches. Though operational units may be more specialized, military and civilian intelligence and security forces in Sweden collect both internal and foreign data. Government and military agencies often coordinate operations, especially in the areas of signals and counterintelligence.

The Military Intelligence and Security Directorate (MUST) oversees Swedish military intelligence operations. The agency coordinates intelligence operations with various specialized military units. The Special Protection Group (SSG) is the military's highly trained intelligence and special forces unit. The SSG protects intelligence and military installations. A Military Police division, with a specially trained covert operations unit called the Military Police Rangers (MPJ), is charged with the protection of military property and defense of national security.

The National Security Service (SAPO) is Sweden's primary government intelligence service. SAPO directs maintains several operational branches, including signals intelligence, counterintelligence, and a national police force. The agency oversees and both foreign and domestic surveillance and analyzes intelligence data. The national police force is the main action unit of the SAPO, and maintains important operational divisions of its own, including the ONI, the Swedish national police counterterrorism unit. The unit has special operational and military action powers to seek out and apprehend terrorists inside Sweden's boarders and throughout Europe, with the aid of foreign intelligence agencies.

In response to growing concern about global terrorism, Sweden joined the European Union international task force to combat terrorism.

SEE ALSO

European Union
Counter-Intelligence

Switzerland, Intelligence and Security

Switzerland has a long tradition of neutrality, abstaining from active participation in World Wars I and II. This policy of neutrality extended to abstaining from membership in international organizations and prohibiting the sharing of some intelligence information with foreign nations. On September 10, 2002, the Swiss Confederation joined the United Nations as a member nation, ending a fifty-five year span as an observer mission. Although Switzerland has cooperated with humanitarian, economic, legal, and intelligence operations with neighboring foreign nations and the United States, it is not a member of the European Union or the North Atlantic Treaty Organization (NATO).

Swiss government agencies, financial institutions, and military branches of service recognize three national languages, German, French, and Italian. Some canton governments use a fourth national language, Romansh. The varied linguistic ethnicities in the country require national services to operate equally in all of its official languages. The multi-lingual nature of the Swiss Confederation and its citizens adds a unique dimension to Swiss intelligence and security forces.

Switzerland's intelligence services effectively dissolved intelligence community distinctions between internal and domestic security and intelligence operations. The recent creation of the Swiss National Security Council, part of the Swiss Federal Department of Defense, Civil Protection, and Sports, facilitated communication and cooperation among various agencies in the intelligence community, giving each independent agency equal access to information and resources. The National Security Council has jurisdiction over civilian and military intelligence and security issues, further uniting various branches of the intelligence community.

The Strategic Intelligence Service is charged with directing and conducting foreign intelligence operations. Its charge is the protection of Swiss banking, economic, political, technological, and military interests abroad. Data collected by the agency is reported to the political and military leadership of the Swiss Confederation via the National Security Council. The Strategic Intelligence Service traditionally works in conjunction with other Swiss agencies, but has increasingly cooperated with adjacent nations in the European Union.

The Armed Forces Intelligence Service trains most Swiss intelligence agents. The agency provides military intelligence units should the army be needed in domestic affairs or called to active duty. Within the armed forces, political and security information is gathered by the Air Force Intelligence Section which conducts internal surveillance of the Swiss intelligence community.

Switzerland's most populous agency in the intelligence community is the Federal Office of Police. The Federal Police are Switzerland's main counterintelligence force, conducting both internal and external surveillance. The Federal Office of Police works closely with other agencies to ensure domestic security.

Syria, Intelligence and Security

Syria has four intelligence agencies, which together helped President Hafez al-Assad maintain strict control of the nation from 1970 to 2000, and assisted the transition of power to his son Bashar after the elder Assad died. Despite the country's reputation as a police state and an exporter of terrorism within the Middle East, Syrian opposition to Iraq and to Islamist groups has often placed it in temporary alignment with United States policies.

The Political Security Directorate (Idarat al-Amn al-Siyasi) conducts surveillance within the country, looking for signs of opposition political activity. Its role overlaps to some extent that of the General Security (or Intelligence) Directorate (Idarat al-Amn al-'Amm), the principal civilian intelligence agency in the country. The latter also has an external security division equivalent to the U.S. Central Intelligence Agency, as well as a Palestine division, which oversees activities of Palestinian groups in Syria and Lebanon.

In addition to the typical functions of military intelligence, the Military Intelligence Service (Shu'bat al-Mukhabarat al-'Askariyya) provides support to Palestinian, Lebanese, and Turkish radical groups, monitors Syrian dissidents living overseas, and coordinates the actions of Syrian and Lebanese forces in Lebanon.

The fourth intelligence service, the Air Force Intelligence Directorate (Idarat al-Mukhabarat al-Jawiyya) is only nominally tied to the air force. Its role as the most powerful and feared intelligence agency in Syria comes from the fact that Hafez al-Assad was once air force commander, and later turned the air force intelligence service into his personal action bureau. In addition to intelligence work, the directorate has assisted numerous terrorist operations abroad.

Despite its reputation, Syria has made common cause with the United States against Iraq, whose Saddam Hussein was a hated foe of Assad, and against militant Islamists. After the U.S. defeat of the Taliban in Afghanistan, extremists ejected from that country began to drift through Syria, but found themselves unwelcome there: the Syrians captured numerous former fighters and held them for questioning by U.S. authorities. In July 2002, U.S. officials

confirmed that Syria's government had provided Washington with information that helped head off a surprise attack on U.S. forces in the Persian Gulf.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

PERIODICALS:

Boyne, Sean. "Assad Purges Security Chiefs to Smooth the Way for Succession." *Jane's Intelligence Review* 11, no. 6 (June 1, 1999): 1.

Schneider, Howard. "Syria Evolves as Anti-Terror Ally." *Washington Post.* (July 25, 2002): A18.

ELECTRONIC:

Syria: Intelligence Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/syria/> (March 1, 2003).

Syria's Intelligence Services: A Primer. Middle East Intelligence Bulletin <http://www.meib.org/articles/0007_s3.htm> (March 1, 2003).

SEE ALSO

Iraq, Intelligence and Security Agencies
Israel, Intelligence and Security
Jordan, Intelligence and Security
Turkey, Intelligence and Security

T

Tabun

Tabun (or "GA") is one of a group of synthetic chemicals that were developed in Germany during the 1930s and 1940s (Tabun was developed in 1936). The original intent of these compounds, including tabun, was to control insects. These pesticides were similar to organophosphates in their action on the nervous system. However, Tabun and the other human-made nerve agents proved to be much more potent than the organophosphates, and so quickly became attractive as chemical weapons.

Tabun is one of the G-type nerve agents, along with Sarin and Soman. They are all clear, colorless, and tasteless. As a result, Tabun mixes readily with water, and so can be used as a water-poisoning agent. Food can also be contaminated. The fluid form of Tabun can also be absorbed through the skin.

When in water, Tabun loses its potency relatively quickly, compared to airborne vapors, which can remain potent for a few days. The vapors can even bind to clothing, where they will subsequently be released for 30 minutes or so. People close to the contaminated person can themselves be affected by the vapor. Tabun vapors tend to be denser than air and so settle into low-lying depressions or valleys. People in such regions are especially susceptible.

Like the other members of the G series, Tabun is a nerve agent. Specifically, it inhibits an enzyme called cholinesterase. The enzyme breaks apart a compound that acts as a communication bridge between adjacent nerve cells. Normally, the transient formation and destruction of the bridge allows a control over the transmission of nerve impulses. But, the permanent presence of the bridging compound means that nerves "fire" constantly, which causes muscles to tire and eventually stop functioning. In the case of the lungs, this can be fatal.

Symptoms of Tabun poisoning, which can begin within minutes of exposure, include runny nose, watery and painful eyes, drooling, excessive sweating, rapid breathing, heart beat abnormalities, and, in severe cases, convulsions, paralysis, and even fatal respiratory failure.

Treatment for the inhalation of Tabun consists of three timed injections of a nerve agent antidote such as atropine. Since this may or may not be successful, prevention remains the most prudent strategy. Protective clothing including a gas mask is a wise precaution for those who are in an environment where the deployment of Tabun is suspected.

While the United States once had an active chemical weapons development program that included the weaponization of Tabun, this program was halted decades ago. Other countries may still be engaged in such weapons development. For example, Iraq is suspected of having used Tabun against Iranians during the Iran-Iraq war in the 1980s.

FURTHER READING:

BOOKS:

Government of the United States. *21st Century Complete Guide to Chemical Weapons and Chemical Terrorism—U.S. Demilitarization Program, Stockpile Destruction Emergency Plans, Nerve Gas and Blister Agent Civilian Treatement and First Aid, Home Sheltering Plans.* Washington, DC: Progressive Management, 2002.

ELECTRONIC:

Agency for Toxic Substances and Disease Registry. "Nerve Agents (GA, GB, GD, VX)." Division of Toxicology, Centers for Disease Control and Prevention. March 13, 2003. <http://www.atsdr.cdc.gov/tfactsd4.html>(April 10, 2003).

Agency for Toxic Substances and Disease Registry. "Facts about Tabun." Division of Toxicology, Centers for Disease Control and Prevention. March 7, 2003. <http://www.bt.cdc.gov/agent/tabun/basics/facts.asp>(April 10, 2003).

SEE ALSO

Chemical Warfare
Mustard Gas
Sarin Gas

Taiwan, Intelligence and Security

For the first four decades after its establishment by ousted Chinese President Chiang Kai-shek in the 1940s, the Republic of China (ROC) or Taiwan was a virtual one-party state ruled by Chiang's Guomindang or KMT. Although its system was capitalist and nominally democratic, the country's people had little freedom of dissent. During those years, the National Security Bureau (NSB) helped maintain Chiang's power by monitoring the citizenry. Liberalization began in the late 1980s, and was reflected in changes by the NSB. Nevertheless, the centralization of the ROC intelligence and security structure remains.

Under the National Security Council (NSC) is the Ministry of Defense, which includes the ROC Army, Navy, Air Force, Coast Guard, and Military Police Command. The Ministry of Defense also has its own Military Intelligence Bureau. Of much greater significance in the intelligence apparatus is NSB, which reports directly to the Ministry of Defense. At one time, its activities were so secretive that it was called "Mystical 110," after the address of its headquarters at 110 Yanteh Boulevard in the Taipei suburb of Yang Ming Mountain. Directed by military leaders, the NSB was known popularly as "Taiwan's KGB" or simply "TKGB." The passage of the NSB Organic Law by the Yuan or national legislature in 1994, however, served to place NSB under a much greater measure of civilian control in the increasingly liberalizing ROC state.

In addition to the NSB is the Ministry of Justice Investigation Bureau (MJIB), which performs functions similar to those of the United States Federal Bureau of Investigation, although its powers are somewhat more broad. Police services are directed by the National Police Administration of the Ministry of Interior. Like South Korea and unlike the United States, Taiwan's police are centrally organized.

FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

PERIODICALS:

Campbell, Kurt M. "Edging Taiwan in from the Cold." *Washington Post.* (April 25, 2001): A31.

Dean, Jason. "Taipei's Turmoil Hinders Action on Key Issues." *Wall Street Journal.* (March 21, 2002): A18.

Li Shaomin. "My Long Journey Home." *Wall Street Journal.* (August 7, 2001): A14.

ELECTRONIC:

Taiwan Intelligence and Security Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/taiwan/> (March 1, 2003).

SEE ALSO

China, Intelligence and Security
Chinese Espionage against the United States
South Korea, Intelligence and Security

Taser

BRIAN HOYLE

A Taser is a type of gun. It is similar in appearance to a conventional gun, having a handle, squeezable trigger, and a blunt barrel. Instead of firing bullets, however, a Taser incapacitates someone for a short time by the use of electricity. Tasers are most often used by security forces, including police, to quell disturbances without causing injury to the people involved.

The Taser gun is one of three types of weapons that are known collectively as stun guns. The other two devices are known as the hand held stun gun and the liquid stun gun. As their name implies, these weapons are designed to be a non-lethal defense, rather than an offensive weapon capable of causing deadly injury.

Stun guns like the Taser operate by disrupting the electrical flow of signals through nerve cells. This electrical flow drives the ability of the muscles to respond to commands from the brain, and allows information that the body receives from the outside world (i.e., touch, taste, smell) to be communicated to the brain. The disruption of the nerve cells is achieved by the generation of an electrical charge by the Taser that has a high voltage and low amperage. Put another way, the electrical charge has a great deal of pressure, but is not intense. The pressure of the charge allows the charge to penetrate into the body, even though several layers of clothing. In order for it to be effective, the person must be close, even in direct contact, with the electrodes of the Taser. Because the electrical charge is not intense, the brief surge of electricity is not powerful enough to physically damage the person's body.

Inside the body, however, the electricity is powerful enough to temporarily disable the nervous system. This occurs when the added charge mixes with the electrical impulses flowing through the nerve cells. The added electricity overwhelms the meaningful signals, making it impossible for the brain to interpret the signals from the

An advanced M-26 Taser stun gun is demonstrated during a news conference in 2002. Several airlines deploy similar weapons on board during flights. AP/WIDE WORLD PHOTOS.

nerve cells. Confusion, difficulty in balance, and muscle paralysis results.

Only about one-quarter of a second is required to incapacitate someone. Once the electrical swamping of the nerve impulses has abated—within a few seconds to a minute—recovery is complete with no adverse effects. Tests have shown that even heart pacemakers are not affected by Tasers.

The electrical signal from a Taser can be generated as a single burst, or in rapid pulses. If the pulses are similar to the frequency of the natural pulses that occur within the nerve cells, then the muscles are stimulated to contract and relax. However, there is no coordination behind the work, since the connections between the muscles and the brain have been disrupted. The muscles will become depleted of energy and tired. Even when the normal electrical rthyhm is restored, the muscles often remain too tired to respond for a short period.

Because a Taser acts on muscles, and as there are muscles all over the body, a Taser applied almost anywhere over the body can cause total immobilization.

Stun guns, including the Taser, consist of a transformer, oscillator, capacitor, and electrodes. The transformer generates the voltage; typically between 20,000 and 150,000 volts. The oscillator introduces the pulsations in the electrical charge. The charge is built up in the capacitor, which releases the charge to the electrodes. It is the electrodes that send the charge into the body, when the electricity bridges the gap between the oppositely charged electrodes.

In a Taser, the electrodes are not fixed in position. Instead, they are positioned on the ends of two long pieces of conducting wire. When a trigger is pulled, a release of compressed gas expels the electrodes out from the gun. In addition, the electrodes have barbs on them, so that they can stick to clothing. This design of the Taser allows a charge to be transferred to someone who is 15 to 20 feet away. Hand-to-hand contact, in this instance, is not necessary. The disadvantage of this design is that only one shot is possible before the electrodes have to rewind, and a new compressed gas cartridge loaded into the gun. Some models of Taser have the attached electrodes, so that if the flying electrodes miss the target, the shooter can move in and try to touch the subject with the stationary electrodes to deliver the stunning dose of electricity.

FURTHER READING:

BOOKS:

Murray, John, James H. Murray, and Barnet Resnick. *A Guide to Taser Technology: Stunguns, Lies, and Videotape.* Dana Point: Whitewater Press, 1997.

ELECTRONIC:

How Stuff Works. "How Stun Guns Work." <http://www.howstuffworks.com/stun-gun.htm>(16 December 2002).

SEE ALSO

Electromagnetic Weapons, Biochemical Effects
Energy Directed Weapons
Less Lethal Weapons Technology

Technical Intelligence

Technical intelligence, or TECHINT, is intelligence relating to the technical abilities of an enemy. It does not fall under just one of the four major branches of intelligence; rather, TECHINT includes elements of imagery, measurement and signatures, and signals intelligence (IMINT, MASINT, and SIGINT, respectively). It may also intersect with the fourth major branch, human intelligence (HUMINT), though some adherents of TECHINT insist that HUMINT plays no part in the gathering of technical intelligence. Closely related to TECHINT is scientific intelligence, or intelligence on the development of new weapons or techniques by an enemy.

Both sides in World War II conducted technical and scientific intelligence operations against one another. For example, the British followed a supply of heavy water, to be used by the Nazis in building an atomic bomb, for several years, and finally destroyed it in transit from Norway to Germany.

Technical and scientific intelligence operations proliferated during the Cold War, along with the many scientific advances that made possible improvements in weapons and surveillance technology. The most notable TECHINT operations were conducted by the Soviets against the United States, as when Julius and Ethel Rosenberg, agents of the Soviet regime, passed nuclear secrets to Moscow.

Much of the reason for the lopsided character of Cold War TECHINT (with the exception of the early space race) was the fact that the United States had far more military and commercial technical expertise to offer than did the Soviet Union. An even greater disparity existed between the United States and the People's Republic of China (PRC) at the end of the twentieth century, when PRC operatives sought to obtain information on U.S. weapons systems and satellites. Much of this material came not as a result of espionage operations, but through open sources.

FURTHER READING:

BOOKS:

Chalou, George C. *Scientific and Technical Intelligence Gathering.* New York: Garland Publishing, 1989.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

Scientists and Engineers: Directorate for Scientific and Technical Intelligence, Directorate for Foreign Intelligence. Washington, D.C.: Defense Intelligence Agency, 1987.

ELECTRONIC:

Army Technical Intelligence Chronology. University of Idaho Library. <http://www.lib.uidaho.edu/technical/techint.html> (April 3, 2003).

SEE ALSO

Chinese Espionage against the United States
IMINT (Imagery intelligence)
Measurement and Signatures Intelligence (MASINT)
Sabotage
Satellite Technology Exports to the People's Republic of China (PRC)
SIGINT (Signals Intelligence)

Technology Transfer Center (NTTC), Emergency Response Technology Program

The National Technology Transfer Center (NTTC) is a research facility on the campus of Wheeling Jesuit University in Wheeling, West Virginia. It was established by Congress in 1989, with a mandate to increase the effectiveness of U.S. industry by providing access to some $70 billion in federally funded research. Among the facilities of this full-service technology management and commercialization center is the Emergency Response Technology (ERT) Program. The latter attempts to match the technology needs of emergency medical, firefighting, hazardous materials, public safety, and special operations personnel with off-the-shelf technologies.

The ERT Program is led by its advisory council, the Emergency Response Technology Group (ERTG). It is the responsibility of the ERTG to identify technology needs and match them to a range of existing technologies. Those existing technologies are evaluated with regard to their applicability to specific areas of need, and assuming it meets the test, the technology is brought before the ERTG as a group to validate it. Upon validating, the ERTG undertakes assistance of the developer by overseeing operational tests and evaluations at participating facilities throughout the United States. Once successfully brought to market, what was once a prototype becomes an operational commercial product.

Among the products the ERTG sought to develop in 2003 was a building and facility emergency response

information/survey tool, which would store data, including location of power panels and wiring, to enhance the ability of rescue personnel to penetrate all areas of a building; a personnel locator/monitor that would provide three-dimensional tracking of emergency personnel at an emergency site; an approaching traffic warning device; and a hazard assessment robot that could be passively activated by remote sensors. In the 18 months prior to September 2002, according to the *Chronicle of Higher Education,* the NTTC as a whole had brokered some 30 deals in which business firms licensed technology developed by the National Aeronautics and Space Administration and the Environmental Protection Agency. An example of a product it had recently helped market was the RoadSpike, a portable device capable of deflating tires of motorists attempting to run roadblocks.

FURTHER READING:

PERIODICALS:

Brainard, Jeffrey. "Profiles in Pork: Wheeling Jesuit University: National Technology Transfer Center." *The Chronicle of Higher Education* 49, no. 5 (September 27, 2002): A23.

Ritchie-Matsumoto, Peggy. "Taking Your Technology to the Marketplace." *Corrections Today* 62, no. 4 (July 2000): 96–100.

ELECTRONIC:

National Technology Transfer Center. <http://www.nttc.edu> (March 18, 2003).

SEE ALSO

Chemical Safety: Emergency Responses
Law Enforcement, Responses to Terrorism
Radiological Emergency Response Plan, United States Federal

Telemetry

Telemetry, from the Greek *tele* (far) and *metron* (measure), is the collection of data using automated sensors that transmit their results to a central monitoring point. A telemetric sensor may be stationary (e.g., fixed on the sea floor) or aboard a mobile platform (e.g., airplane, spacecraft, missile, submarine). The quantities sensed are usually simple variables that can be reported at regular intervals, such as temperature, pressure, humidity, altitude, fuel level, battery voltage, salinity, vibrational intensity, alarm status, or the like. Complex, high-speed signals such as video are usually not termed telemetry, even when they are collected remotely by unattended devices.

The raw output of a remote sensor is often an analog signal, that is, a voltage or current that varies smoothly with time. Before transmission, such a signal is usually converted to digital form by the process of analog-to-digital conversion or sampling. In sampling, an analog signal is examined at evenly-spaced moments and a binary number assigned to its magnitude; the larger the sensor output, the larger the binary number. The raw bitstream produced by sampling is organized by the telemetry device into standard-length frames containing added information specifying data type, time of acquisition, and so forth. If the transmission channel is noisy, the signal may also be subjected to error-correction coding to allow recovery of data from errors. The signal may also, in some military applications, be encrypted before transmission. The final telemetry signal is sent from the data-collection point using radio, sonar, coaxial cable, or some other medium to a receiving station, where it is recorded and monitored by computers or human operators.

Telemetry is employed for many purposes throughout the commercial, scientific, and military sectors. For example, controllers of missiles, torpedoes, spacecraft, or remotely piloted aircraft such as the Predator require access to numerical information of many sorts in order to monitor and adjust the performance of these complex machines. Telemetric data may also be used for surveillance purposes, as when deep-sea acoustic sensors are used to track submarine movements, and is essential to the control of spacecraft, whether crewed or robotic.

FURTHER READING:

ELECTRONIC:

Wilson, Elizabeth. *Introduction to AMMOS Telemetry Processing.* Jet Propulsion Laboratory, NASA. October 18, 2001. <http://tel.jpl.nasa.gov/~betsy/mm/intro.htm> (Nov. 14, 2002).

SEE ALSO

Cipher Pad
Codes and Ciphers

Telephone Caller Identification (Caller ID)

Caller identification, or caller ID, permits the receiver of a call to identify the caller's location. Available since the early 1990s, it has enhanced the sense of privacy enjoyed by persons in their homes, and has also greatly reduced the number of prank calls, as well as calls made with threatening or criminal intent. Ambivalence about the privacy ramifications of caller ID, however, has made the state of California slow to accept the technology.

In 1985, the *Los Angeles Times* ran a report on an ultra-chic security products boutique whose customers included the late Shah of Iran and the makers of the James Bond movies. Counter Spy Shop (CSS) in Washington, D.C., sold a telephone voice scrambler for $14,000, yet, as the newspaper article noted, "What CSS cannot do, despite numerous requests from potential customers, is pinpoint the place of origin of an incoming call." To do so "would require access to the telephone company's computers, something that even CSS lacks."

Within half a decade, telephone companies had made such technology available, for a small fee, to all customers. A caller ID box, or a caller ID unit built into a phone, simply reads the computerized information for the incoming call, assuming it is coming from a listed number. Calls from an unlisted number register as "Unknown Caller" or "Private Caller." Available on internal private branch exchange (PBX) telephone systems during the 1980s, caller ID gained use by businesses offering toll-free numbers in 1988. It became available to residential customers in 1989, and by 2001, 43% of homes nationwide had caller ID.

An exception was California, where privacy concerns had kept the service away for many years. Before telephone companies could bring caller ID into the state, they had to spend $34 million on an advertising campaign to tell callers that the service would make their phone numbers visible, and that this could be used to obtain the caller's address. By 2001, four years after the introduction of caller ID in the state, about one quarter of Californians used the service.

■ FURTHER READING:

PERIODICALS:

Crabb, Peter B. "The Use of Answering Machines and Caller ID to Regulate Home Privacy." *Environment and Behavior* 31, no. 5 (September 1999): 657–70.

Kupperschmid, David. "James Bond 'Supplier' Has the Cure for Whatever Is Bugging You." *Los Angeles Times.* (April 26, 1985): 2.

MacSweeney, Greg. "Caller ID with a Kick." *Insurance & Technology* 25, no. 10 (October 2000): 30–35.

Mehta, Stephanie N. "Playing Hide-and-Seek by Telephone—Phone Companies Are Arming Both Sides in the Battle to Screen Unwanted Callers." *Wall Street Journal.* (December 13, 1999): B1.

"Tech 101: Hollywood's Caller ID Hang-Up." *Los Angeles Times.* (May 24, 2001): T1.

ELECTRONIC:

Johnson, Jeff. Caller Identification: More Privacy or Less?—Winter-Spring 1990 (Volume 8, Number 2). Computer Professionals for Social Responsibility. <http://www.cpsr.org/publications/newsletters/issues/2001/summer/jj.html> (April 2, 2003).

SEE ALSO

Privacy: Legal and Ethical Issues
Telephone Scrambler

Telephone Recording Laws

In the United States, each state has its own laws regarding the recording of phone calls, while recording of interstate calls is governed by federal law, most notably the Federal Wiretapping Act. In some cases, taping is legal with the consent of both parties, but the laws can be complex and open to arcane interpretations. Recording of conversations has played an important role in American political and legal history, from Watergate and other presidential scandals to lesser-known cases.

President Richard M. Nixon's illegal taping of private conversations figured prominently in the Watergate scandal of the early 1970s, although in fact, presidents have been recording conversations for as long as such technology has been available. In the Clinton-Lewinsky scandal, involving President William J. Clinton's sexual relationship with White House intern Monica Lewinsky and his attempts to cover it up, key evidence came from conversations between Lewinsky and her friend Linda Tripp—conversations Tripp recorded without telling Lewinsky. Such was the depth of Americans' resentment toward the threat of privacy invasion (combined with popular liking for the affable Clinton) that Tripp become the focus of far greater condemnation than did the President.

In 1997, secretly made tapes of Texaco executives furnished proof of racial discrimination, and led the company to settle a $176 million lawsuit.

Although Justice Louis Brandeis described wiretapping as "evil" in *Olmstead v. United States* (1928; 277 U.S. 438), the federal government has, in the view of many civil liberties groups, at best a questionable record in this area. Since the 1970s, a backlash against domestic surveillance and intelligence efforts has reduced the power of the Federal Bureau of Investigation and other law-enforcement authorities in this area. As for telephone recording by individuals, this is subject to some form of criminal penalty in all 50 states, and at the federal level. However, the Federal Wiretapping Act does allow telephone service providers, business owners, and consenting parties to record calls under certain circumstances.

■ FURTHER READING:

PERIODICALS:

Cloud, David S., and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal.* (April 5, 2000): A4.

Halbfinger, David M. "Mother and Lawyer Charged in Sale of 10-Week Old Baby." *New York Times.* (March 30, 1999): 4.

McCarter, Kimberly M. "Tape Recording Interviews." *Marketing Research* 8, no. 3 (fall 1996): 50–51.

Skoning, Gerald. "Be Careful Not to 'Tripp'." *HR Magazine* 43, no. 6 (May 1998): 125–30.

SEE ALSO

Domestic Intelligence
Foreign Intelligence Surveillance Court of Review
Privacy: Legal and Ethical Issues
Telephone Recording System
Telephone Tap Detector

Telephone Recording System

A telephone recording system can be as simple as a handheld phone receiver with an analogue (non-computerized, non-digital) recorder. In such a situation, the act of recording is hard to hide. On the other hand, some telephone recording systems are so seamless that the individual being recorded would not known unless informed. For this reason, some states require that the person being recorded be informed of this fact, and many states require that the recorder emit a regular beep or other sound to serve as a reminder of the ongoing recording.

Consumers today are able to buy telephone recording systems that hook into the telephone line just as an answering machine would. Such systems, which retail from under $100, make it possible to begin recording as soon as the receiver is lifted. Twelve states require "two-party notification," meaning that both participants in a recorded conversation must be informed of the fact that they are being recorded.

In California, laws further require that the recording equipment continually emit a beeping tone so as to maintain awareness of the recording process. Sophisticated consumer recording systems can be configured in such a way as to play the beep if necessary. Digital systems are even capable of saving a recorded call in a digital audio format, as a .wav file, making it possible for a user to e-mail a recording of a conversation.

■ FURTHER READING:

PERIODICALS:

Cloud, David S., and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal.* (April 5, 2000): A4.

McCarter, Kimberly M. "Tape Recording Interviews." *Marketing Research* 8, no. 3 (Fall 1996): 50–51.

Skoning, Gerald. "Be Careful Not to 'Tripp'." *HR Magazine* 43, no. 6 (May 1998): 125–130.

SEE ALSO

Domestic Intelligence
Privacy: Legal and Ethical Issues
Telephone Recording Laws
Telephone Tap Detector

Telephone Scrambler

A telephone scrambler encrypts phone conversations, keeping unauthorized users from tapping into or monitor calls with any success. Scrambling involves the encryption of data, using unique codes that render it possible only for authorized personnel to unscramble transmissions. In order for scrambling technology to work, it is necessary that both authorized participants in a conversation possess a scrambler/descrambler. Scramblers are available on the consumer market, but most of these are vastly inferior to the technology used by operatives of elite U.S. intelligence services.

In a phone scrambling system, information sent over a public switched telephone network, or PSTN, is scrambled. The authentication of the unscrambling device at the receiving end is checked, and when an incoming message is received, it remains inaccessible until a special code or identification number is entered. One consumer system, according to a report in the trade journal *Security,* uses voice coding technology as a further security measure.

The principle of telephone scrambling is similar to that applied in making a Web site secure so that users can enter financial information without fear that this data will be intercepted. In both cases, sophisticated encryption makes it all but impossible for interlopers to obtain the desired information.

It is a safe bet that decryption technology and techniques available to an upper-echelon intelligence organization such as the National Security Agency, on the other hand, could easily break into even the best civilian systems. Likewise, U.S. intelligence services in hostile environments such as Iraq during the 2003 war have at their disposal telephone scrambling and decryption technology that would make their transmissions virtually impenetrable.

■ FURTHER READING:

PERIODICALS:

Baldauf, Scott. "Where to Find the Perfect Gift for Your 007 Wannabe." *Christian Science Monitor.* (December 7, 1999): 2.

"How Secure Are Your Phone, Fax, Data Transmission Systems?" *Security* 34, no. 6 (June 1997): 75–76.

Nolte, Carl. "Spy Store a Boon for Paranoid Public." *San Francisco Chronicle.* (January 18, 2002): A23.

SEE ALSO

Domestic Intelligence

Encryption of Data
Privacy: Legal and Ethical Issues
Telephone Tap Detector

Telephone Tap Detector

A telephone tap detector aids communication security by providing electronic recognition of attempts to intercept a call through wiretapping or listening devices. Telephone tapping is, at least in certain particulars, an exact science, and tap detection technology must likewise be efficient to counteract those efforts. With telephone tapping no longer an extremely infrequent aspect of daily life, tap detectors have become a popular item among security-conscious consumers.

In tapping into a phone line, surveillance personnel use technology akin to that which an electrician might apply in attempting to siphon power from an electric line. However, whereas an electric wire attached to a circuit receives a regular supply of power, a telephone tap cannot maintain constant access to a telephone line, or it would be too easy to detect. Instead, the tap actually "seizes" the telephone line as a call is coming in.

The tap is most likely to engage between the first and third ring of an incoming call, and from that point onward, assuming all conditions are reasonably favorable for surveillance, the tap remains in effect for the duration of the call. A telephone tap detector recognizes this seizure of the phone line, and provides further verification once the call concludes. Depending on the number and timing of disconnection reactions after the receiver is reengaged, a good tap detector (consumer models sell for several hundred dollars) can determine whether wiretapping equipment is in the process of disengaging from the phone line.

FURTHER READING:

PERIODICALS:

Cloud, David S. and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal.* (April 5, 2000): A4.

"How Secure Are Your Phone, Fax, Data Transmission Systems?" *Security* 34, no. 6 (June 1997): 75–76.

Kupperschmid, David. "James Bond 'Supplier' Has the Cure for Whatever Is Bugging You." *Los Angeles Times.* (April 26, 1985): 2.

"Texas Politicians' Cases Prompt New Interest in Eavesdropping." *San Francisco Chronicle.* (December 18, 1995): A12.

SEE ALSO

Domestic Intelligence
Foreign Intelligence Surveillance Court of Review
Laser Listening Devices
Privacy: Legal and Ethical Issues
Telephone Recording Laws
Telephone Recording System
Telephone Scrambler

Terror Alert System, United States

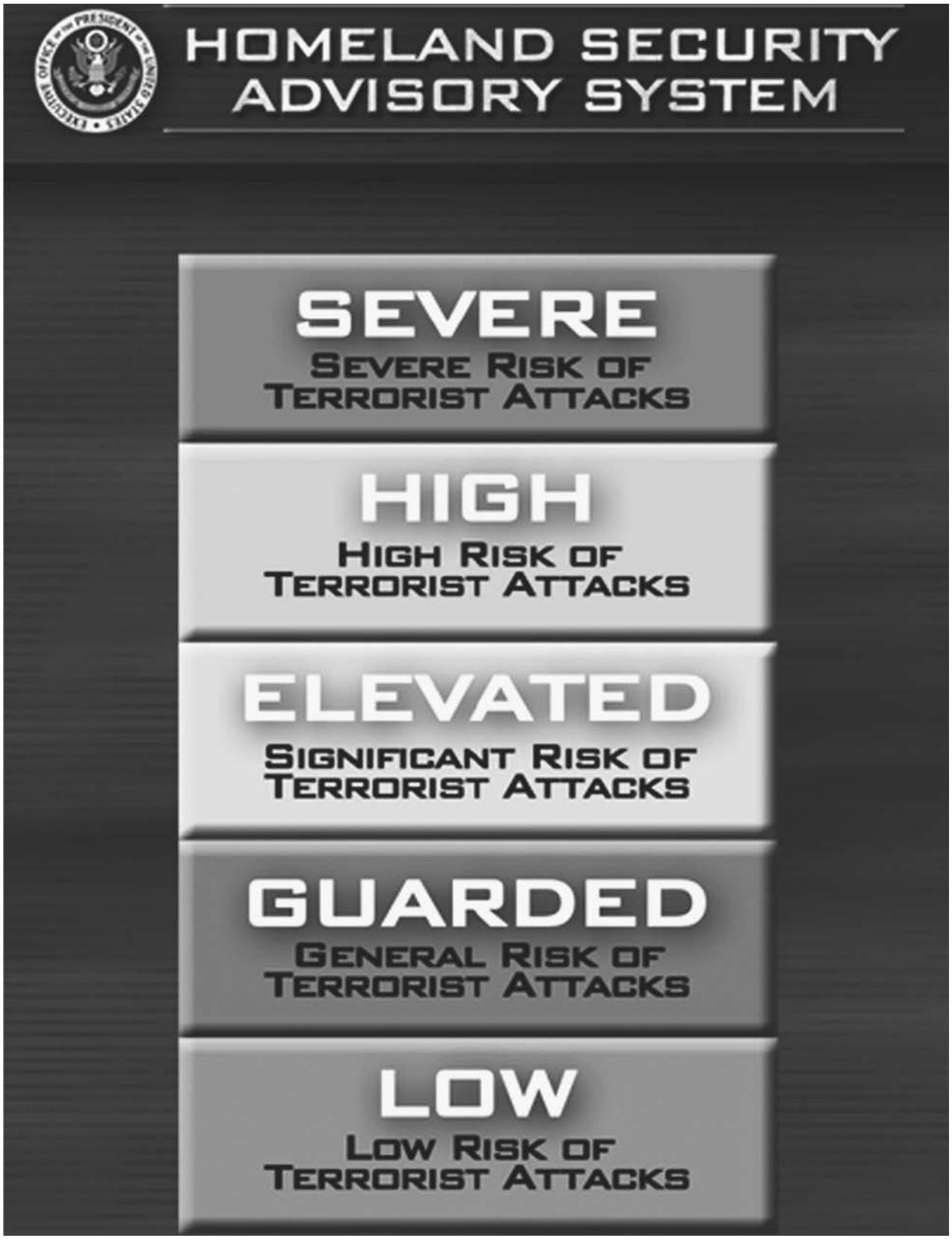
JOSEPH PATTERSON HYDER

On March 12, 2002, President Bush created the Homeland Security Advisory System (HSAS) by signing Homeland Security Presidential Directive 3. The HSAS is a five-tiered alert system designed to quickly notify government agencies, industry, and the public about terrorist threats to United States interests at home and abroad. The White House established the HSAS under the Attorney General's office in conjunction with the Office of Homeland Security, but the Department of Homeland Security (DHS) now controls the HSAS. The goal of this color-coded alert system is to increase effective communication and cooperation among the various federal, state, and local agencies that would be involved in the event of a terrorist attack and to make the public more aware of the threat of a terrorist attack.

Before the establishment of the HSAS, numerous federal and local agencies utilized their own threat level assessments. These threat level assessments were used to notify specific agencies or sectors of government about possible attacks on American interests. The federal agencies that made such assessments did not readily disseminate this information to the American public or to state and local governments. Various agencies also acted on different intelligence reports, leading to disparate threat assessments. The HSAS provides a framework for these various alert systems.

One of the most publicized components of the HSAS is its color-coded warning system. This system consists of five Threat Conditions, each accompanied with suggested Protective Measures. The five Threat Conditions are Low (Green), Guarded (Blue), Elevated (Yellow), High (Orange), and Severe (Red). The DHS and Attorney General devised the HSAS to provide an easy way for local governments and the public to assess the current situation and take appropriate action.

The Department of Homeland Security has also devised a set of recommended actions, or Protective Measures, for local governments, industry, and the public to follow based on the alert level. These recommendations include increased security for public events, increased



The five-level, color-coded terrorism warning system, enacted in 2002, is a response to public comments that broad terror alerts issued by the government raised alarm without providing useful guidance. AP/WIDE WORLD PHOTOS.

surveillance, and implementation of local emergency response plans.

The Department of Homeland Security defines the Low Condition (Green) as indicating a low risk of terrorist attacks. Under the Green level, government agencies and private industry should train personnel and analyze emergency plans. The Guarded Condition (Blue) indicates a general risk of terrorist attacks. Protective Measures dictate updating emergency procedures and keeping the public informed. The Elevated Condition (Yellow) signals a significant risk of terrorist attack. Under this condition, surveillance of sensitive locations is increased and emergency plans are readied and implemented, when necessary.

The Department of Homeland Security declares a High Condition (Orange) when specific and collaborated information indicates a significant risk of terrorist attack. Under an Orange alert, security is tightened at high-profile public events, and the events are cancelled, if necessary. Access may also be restricted to sensitive areas, such as dams, nuclear power facilities, and government buildings. A Severe Condition (Red) signifies a severe risk of terrorist activity. A Red alert is only declared when there is a real and significant threat. Emergency personnel are reassigned as needed, transportation is closely monitored or redirected, and public facilities may be closed.

Critics of the HSAS assert that the Threat Conditions system claim that the color-coded Threat Conditions may actually be detrimental to national security. These critics claim that the DHS holds the Threat Conditions at an artificially high level in order to give the appearance of preparedness and to avoid public outcry if a terrorist attack occurred at a low threat level. In addition, critics contend that leaving the color-coded warning at an artificially high level will erode public trust in the system.

The Department of Homeland Security counters its critics by maintaining that elevating the Threat Condition when warranted deters terrorism by showing that America is vigilant. Additionally, an elevated Threat Condition alerts law enforcement to increase its efforts to combat terrorism. The Department of Homeland Security also has set criteria for raising or lowering the Threat Condition. The DHS weighs the credibility, specificity, and gravity of every piece of intelligence that is interpreted as a potential threat. The DHS, in conjunction with the FBI, CIA, and other agencies, then seeks to corroborate specific threats. Based on their findings, the DHS will then raise or lower the Threat Condition either for the entire nation or for a specific region.

FURTHER READING:

ELECTRONIC:

United States Department of Homeland Security. <http;// www.dhs.gov> (May 2003).

SEE ALSO

Homeland Security, United States Department

Terrorism, Domestic (United States)

JUDSON KNIGHT

The U.S. Federal Bureau of Investigation (FBI) defines domestic terrorism as terrorism involving groups based in, and operating entirely within, the United States and its territories, without foreign direction. The FBI further divides domestic terrorism into three basic categories: right-wing, left-wing, and special-interest terrorism. Terrorist organizations in the United States had their beginnings with the foundation of the Ku Klux Klan in 1866. White racist movements remain major contributors to terrorism, but the toll of terrorist activities has also included socialist, anarchist, and minority nationalist groups, as well as terrorism associated with the environment and animal rights. Of the 205 lives claimed in terrorist incidents within the United States between 1980 and 1999, more than 80% died in a single attack: the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995.

Domestic Terrorist Groups

At the center of domestic counterterrorism efforts is the FBI, whose Counterterrorism Division defines domestic terrorism thus in a 1999 report titled *Terrorism in the United States:*

"Domestic terrorism involves groups or individuals who are based and operate entirely within the United States or its territories without foreign direction, and whose acts are directed at elements of the U.S. government or population. Domestic terrorist groups can represent right-wing, left-wing, or special interest orientations. Their causes generally spring from issues relating to American political and social concerns."

Right-wing terrorism. Right-wing terrorist groups, as defined by the FBI, are motivated by notions of white racial supremacy, as well as anti-government and anti-regulatory beliefs. They may also include extremist Christian groups such as those that bomb abortion clinics, although these groups are sometimes lumped in with special-interest terrorists. Moreover, many acts of right-wing terrorism, such as racially motivated attacks by "skinhead" gangs, are legally classified as hate crimes rather than domestic terrorism. They thus fall within the realm of the FBI Criminal Division, rather than the Counterterrorism Division.

Not all anti-government groups are necessarily racist: for example, some members of the militia movement in the 1990s attempted to distance themselves from anti-black and anti-Semitic hate groups. On the other hand, all

these groups are united by a suspicion of, or hatred for, the federal government, often coupled with a conspiratorial view of history and politics. These putative conspiracies may have their origins in Washington—which, in the view of many right-wing terrorist groups, seeks to take away Americans' guns and impose ruinous taxes and regulations on them—or they may be international in origin. Many of these groups in the 1990s, for instance, spoke of black helicopters supposedly operated by United Nations forces on U.S. soil.

The Ku Klux Klan. Strictly speaking, the Ku Klux Klan is not a terrorist organization, as its acts of violence have tended to be retaliatory rather than symbolic. Still, given its influence on events in the United States, no discussion of right-wing terrorism would be complete without its mention

Formed by ex-Confederate soldiers after the Civil War, the Klan was an attempt to strike back at the federal government for its imposition of martial law and military occupation in the South. However, the victims of Klan violence—recently freed slaves—were far more vulnerable than the Southern whites, no matter how disenfranchised and dispossessed as they might have seen themselves to be. The Klan, which terrorized and killed African Americans throughout the South, was outlawed by the Ku Klux Klan Act of 1871. In 1882, the U.S. Supreme Court declared the Klan Act unconstitutional, but by then Reconstruction was over, and the Klan had faded into the background.

D. W. Griffith's 1915 film *Birth of a Nation* helped influence the formation of a new Ku Klux Klan at Stone Mountain, Georgia. Over the next decade, the Klan grew in strength nationwide, and prominent persons—including future U.S. Supreme Court Justice Hugo Black—belonged to the organization. Ironically, it was the Klan in 1925, before Martin Luther King, Jr., was born, who undertook the first major "March on Washington" of the twentieth century.

During the 1950s and 1960s, Klansmen conducted terrorist attacks and acts of murder against African Americans and civil rights workers, but the triumph of the civil rights movement spelled the end of the Klan as a force. In the 1970s and 1980s, the Southern Poverty Law Center and other anti-racist organizations successfully gutted the Klan with a series of lawsuits. With its assets stripped, the organization split into numerous splinter groups.

Other racist groups. Alongside Klan movements have been other racist groups, most notably the American Nazi Party (whose founder, George Lincoln Rockwell, was assassinated in 1967 by a member of his own party) and various "Aryan" organizations such as the White Aryan Brotherhood and the Aryan Nations. These groups have often found themselves confronted with a contradiction. Persons on the right, even the extreme right, tend to be patriotic, if sometimes ambivalent about the government in power, whereas Nazi and Aryan groups ultimately pay homage to one of America's most hated historical enemies, Adolf Hitler.

On the other hand, many racist groups, such as the White Patriot Party, have built the "patriot" theme into their name. Others, such as the so-called "Christian Identity Movement" (whose members reject that name) identify white America with the 10 lost tribes of Israel. The Christian Identity Movement and other such groups are profoundly anti-Semitic. None of these groups is, in strict terms, a terrorist group (though they are certainly classifiable as hate groups), but as with the Klan, discussions of right-wing terrorism require reference to such groups.

The bible for adherents of white racist and anti-government belief systems is not Hitler's *Mein Kampf,* but a distinctly American version, more dime novel than political manifesto. This is *The Turner Diaries* by Andrew MacDonald, a.k.a. William Pierce. Published in 1978, the novel pictures a race war that results in the triumph of whites over blacks, Jews, and other "mongrels." It identifies April 20, 1999, as the 110th birthday of "The Great One" (Hitler was born April 20, 1889), and depicts a terrorist bombing of a government building that seems to have provided Oklahoma City bomber Timothy McVeigh with a model for his attack.

Anti-government groups. The remainder of right-wing terrorist groups are united by an anti-government stance that may or may not also embrace racism. Such groups emerged on the national scene with a February 13, 1983, attack on law enforcement officers in Medina, North Dakota, by a group named the Sheriff's Posse Comitatus.

The years since have seen a proliferation of groups such as the various "militias" (anti-government paramilitary groups organized at a state level) or the Freemen. Some of these engage in terrorism by other means, such as the filing of bogus liens and other groundless legal claims that tie up government resources. Sometimes referred to as "paper terrorism," these acts clogged up courts in some western states during the 1990s.

Just as the Klan had a natural base in the South, and some racist groups have found a home in the Midwest (for instance, the American Nazis, which operate primarily in Chicago), the wide-open spaces of the West have provided a natural venue for anti-government groups and individuals. Many of these reacted strongly to the 1992 FBI raid against the Ruby Ridge, Idaho, residence of white separatist Randy Weaver, which resulted in the death of Weaver's wife and son.

The presidency of William J. Clinton proved particularly odious to anti-government groups and individuals, who perceived the Clinton administration as leftist. Anti-government groups claimed that Attorney General Janet Reno was to blame for the April 19, 1993, attack on the Waco, Texas compound of the Branch Davidians, a religious sect reportedly hoarding a cache of illegal weapons.

After a 51-day siege by the Bureau of Alcohol, Tobacco, and Firearms, a combined FBI and Delta Force team assaulted the compound, whereupon the Branch Davidians set the buildings on fire. Seventy-six people, including cult leader David Koresh, died in the conflagration. Outside the compound, a group of anti-government protesters, which had been keeping vigil for weeks, watched as the blaze erupted. Among those present was a 25-year-old Persian Gulf War veteran named Timothy McVeigh.

Oklahoma City. Exactly two years after the Waco incident, at 9:02 a.m. on April 19, 1995, a Ryder rental truck parked in front of the Murrah Federal Building in Oklahoma City exploded. Inside the truck was a 4,800-pound bomb of ammonium nitrate and fuel oil, a combination similar to that used in the 1993 World Trade Center blast. The blast tore a hole along the side of the nine-story building, injuring some 500 persons and killing 168—including 19 infants in a day-care center.

Within minutes, word began to spread throughout the nation that—in a variation on language that would often be used by members of the media in the next few days—"terror had struck the heartland." Authorities already had two suspects, who they had named "John Doe No. 1" and "John Doe No. 2," and initially many reporters speculated that Muslim extremists had caused this blast, as they had the World Trade Center bombing. The men ultimately charged for the Oklahoma City bombing, however, would turn out to be from much closer to home.

About 90 minutes after the blast, police in Perry, Oklahoma, stopped McVeigh for driving without a license plate. When they searched his trunk, they discovered anti-government literature, along with significant traces of PETN, a compound used in the making of the bomb. Soon afterward, having recovered the vehicle identification number of the Ryder truck from its axle, authorities traced it to a rental outlet in Junction City, Kansas, where the owner identified McVeigh as the man who had rented the truck under the name "Robert Kling." McVeigh also matched the composite sketch of "John Doe No. 1."

On April 21, federal authorities arrested McVeigh, along with brothers Terry and James Nichols. James was later released, but McVeigh and Terry Nichols stood trial. Although McVeigh had been involved with the militia movement for a time, he had long since separated himself from any group. His philosophy was strongly anti-government, and it appears that he chose the Murrah Building because he thought (incorrectly) that the personnel involved at Waco worked in that building.

Both McVeigh and Nichols were found guilty, and McVeigh was given the death penalty, while Nichols received a life sentence without parole. McVeigh was executed on June 11, 2001. Exactly three months later, the foreign-sponsored terrorist attacks in New York City, Washington, and Pennsylvania, would eclipse the Oklahoma City death toll by a factor of nearly 20.

Left-Wing and Special Interest Terrorists

So great has been the impact of right-wing terrorism, due to the Oklahoma City bombing (as well as the visibility of hate groups such as the Klan and neo-Nazis), that the significance of left-wing and special interest terrorism has tended to be obscured. In these cases, the death toll is much smaller, but a number of incidents have claimed lives and property.

Left-wing terrorists, according to the FBI, have a revolutionary socialist agenda, and present themselves as protectors of the populace against the alienating effects of capitalism and U.S. imperialism. Notable early participants in left-wing terrorism were various socialist and anarchist groups from the late nineteenth and early twentieth centuries. Leon Czolgocz, who shot President William McKinley in 1901, embraced anarchist beliefs, though no anarchist group would accept him for membership.

Puerto Rican nationalists. From the 1950s, Puerto Rican nationalists have been among the most prominent left-wing terrorists. These might seem at first glance to have a special-interest agenda, but due to their socialist rhetoric and goals, the FBI has categorized them as left-wing terrorists. On November 1, 1950, members of the Puerto Rican Nationalist Party attempted to assassinate President Harry S Truman, and during the 1950s, members of the group stormed the U.S. House of Representatives.

On May 1, 1961, Puerto Rican-born Antuilo Ramierez Ortiz hijacked a National Airlines flight and diverted it to Havana. This was the first successful hijacking of a U.S. plane, and Ortiz, who returned to the United States in 1975, was sentenced to 25 years for his crime. On January 27, 1975, members of the Armed Forces for Puerto Rican Liberation (known by its initials in Spanish, FALN), bombed a bar on Wall Street in New York City, killing four and wounding 60.

The late 1960s and early 1970s. Two days after the FALN attack, members of the Weather Underground claimed responsibility for a bombing at the U.S. State Department in Washington, D.C. The "Weathermen," as they were commonly known (after a line from the song "Subterranean Homesick Blues" by Bob Dylan), were formed from the radical Students for a Democratic Society group in 1969. Their leaders received training in Havana, and over the next few years, they conducted a wave of bombings and robberies. Their death toll was small, however, and consisted primarily of three group members killed when a bomb they were building accidentally exploded at a Greenwich Village townhouse in March 1970.

The late 1960s and early 1970s was also the heyday of the Black Panther Party and other African American nationalist groups that used terrorist tactics. Among the

most notorious events associated with the Black Panthers was an August 7, 1970, raid on a California courthouse by University of California professor Angela Davis and Jonathan Jackson on behalf of Jackson's imprisoned brother George. Davis and Jackson kidnapped several people, critically wounded a district attorney, and killed a judge. Jackson died in the struggle, and on August 21, 1971, George Jackson died in a prison riot he incited after his lawyer reportedly smuggled a pistol to him.

Also notable among left-wing groups of the era was the Symbionese Liberation Army (SLA), which on February 5, 1974, kidnapped heiress Patricia Hearst. Formed in 1973, the group declared war on "fascism," which it equated with America, and it waged its war primarily through bank robberies. Hearst, allegedly brainwashed by the group, adopted the name "Tania" and participated in the robberies. Most of its members, including leader Donald DeFreeze, were killed in a May, 1974, shootout with authorities. Hearst was captured by the FBI in September, 1975. In January, 2001, outgoing president Clinton pardoned her, along with several Puerto Rican revolutionaries held in federal prisons.

Rudolph and Kaczynski. Special-interest terrorism, as its name indicates, is focused on specific issues. Such terrorism tends to be predominantly left-wing, but there are exceptions, most notably the acts attributed to Eric Robert Rudolph. These might be classified as right-wing attacks, as the bombing targets included abortion clinics and a nightclub frequented by homosexuals. On the other hand, the bombing at Atlanta's Centennial Olympic Park on July 27, 1996, during the 1996 Olympics, an attack that killed two people and injured 112, is not currently tied to an obvious political agenda. As of mid-2003, Rudolph had evaded capture, and remained on the FBI's "Ten Most Wanted" list.

Also difficult to classify are the crimes of Theodore Kaczynski, the accused Unabomber. Beginning in 1978, when a bomb disguised as a package went off at Northwestern University, a mysterious bomber terrorized universities and airlines (hence the name *una* in the nickname given to him by the FBI). After a total of 10 attacks on universities and airlines, the Unabomber struck a computer store in Sacramento, California, on December 11, 1985, causing his first fatality.

The Unabomber was spotted on February 20, 1987, placing a bomb at another computer store, this one in Salt Lake City, Utah. This sole sighting provided authorities with a sketch of the Unabomber, who then ceased activities for six years. In June 1993, after two more bombings that month, the Unabomber sent the *New York Times* a letter outlining an agenda based in environmental and anarchist themes. His last two attacks, in 1994 and 1995 (the latter just five days after Oklahoma City) struck an advertising executive and a timber industry lobbyist respectively, again suggesting an anti-capitalist, environmentalist agenda.

After reading the Unabomber's manifesto, David Kaczynski noted similarities between the writer and his brother Ted, and alerted authorities. Ted Kaczynski, once a promising mathematics graduate student, had abandoned society for the isolation of a cabin in Montana, where he was arrested on April 3, 1996. In January 1998, on the eve of his trial, a judge rejected Kaczynski's request to represent himself in court. Kaczynski filed a guilty plea, and was sentenced to life in prison. Though Kaczynski's acts seem terroristic, inasmuch as they are arguably directed at human beings as symbols rather than purely as humans, the FBI did not officially classify his bombings as domestic terrorism, noting a "lack of information regarding the subject's motivation."

Special-interest terrorism in the 1990s. In the 1990s, special-interest terrorism of the political right included attacks and threats against abortion clinics. Special-interest terrorism on the political left involved motivations that included the environment, animal rights, and opposition to globalization. The FBI paid special note to the left-wing groups in this instance, not because of political bias, but because attacks on abortion clinics are classified as hate crimes, giving them an entirely different legal definition and involving other arms of the national justice system.

On the other hand, the acts of groups such as the Animal Liberation Front (ALF) or the Earth Liberation Front (ELF) fit within the FBI's definition of terrorism. The ALF, affiliated with similar groups worldwide, conducts raids on research laboratories and other facilities where, in the view of group members, animals are mistreated. Radical environmentalists have been charged with "tree spiking," or putting metal spikes in trees to harm loggers who cut them, and of mailing packages rigged with razor blades. In October 1998, the ELF was charged with setting fire to a ski resort in Vail, Colorado.

The FBI also noted the rise of anti-globalization demonstrations, which are founded in an opposition to the growth and international influence of Western corporations and financial entities. Though officially grouped with left-wing terrorism because of its strongly anarchist undertones, anti-globalization activities might also be considered special-interest in nature. During the World Trade Organization ministerial meetings in Seattle from November 30 to December 3, 1999, anti-globalization demonstrators conducted extensive acts of vandalism.

CONPLAN

On June 21, 1995, just two months after the Oklahoma City bombing, President Clinton issued Presidential Decision Directive (PDD) 39, "U.S. Policy on Counterterrorism." Its purpose was to provide guidelines for deterring terrorism on America's shores, as well as terrorism against Americans and allies abroad. In accordance with PDD 39 and PDD 62, issued the same day, U.S. government agencies developed the United States Government

Interagency Domestic Terrorism Concept of Operations Plan, or CONPLAN for short.

Presented in January 2001, CONPLAN outlines the response to a domestic terrorist attack, or a foreign-sponsored terrorist attack on U.S. soil, such as those that occurred eight months later, on September 11. CONPLAN identifies the FBI as the lead agency for domestic counterterrorism, and the Federal Emergency Management Agency (FEMA) as the lead consequence management agency. It also outlines responsibilities for the Attorney General and Department of Justice, FEMA, the Environmental Protection Agency, and the departments of Defense, Energy, and Health and Human Services.

■ FURTHER READING:

BOOKS:

Abanes, Richard. *American Militias: Rebellion, Racism, and Religion.* Downers Grove, IL: InterVarsity Press, 1996.

Ellis, Richard J. *The Dark Side of the Left: Illiberal Egalitarianism in America.* Lawrence, KS: University Press of Kansas, 1998.

George, John, and Laird Wilcox. *American Extremists: Militias, Supremacists, Klansmen, Communists, and Others.* Amherst, NY: Prometheus Books, 1996.

Terrorism in the United States 1999. Washington, D.C.: Federal Bureau of Investigation, 1999.

SEE ALSO

Architecture and Structural Security
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)
Coordinator for Counterterrorism, United States Office
Domestic Emergency Support Team, United States
Domestic Intelligence
Domestic Preparedness Office (NDPO), United States National
FBI (United States Federal Bureau of Investigation)
GAO (General Accounting Office, United States)
General Services Administration, United States
Terrorism, Intelligence Based Threat and Risk Assessments
Terrorism, Philosophical and Ideological Origins
Terrorism Risk Insurance
Terrorist and Para-State Organizations
Terrorist Organizations, Freezing of Assets
Terrorist Threat Integration Center
United States, Counter-Terrorism Policy

Terrorism, Intelligence Based Threat and Risk Assessments

■ JUDSON KNIGHT

In the 1990s, a terrorism risk assessment conducted by the General Accounting Office (GAO) led to preparedness recommendations for United States municipalities. By May 1998, GAO reported, only 11 cities had put in place the necessary emergency response systems. Intelligence-based terrorism threat and risk assessments gained much greater import after the terrorist attacks of September 11, 2001, but the U.S. intelligence community often found itself in the challenging situation of recommending public warnings without inciting panic or alternately, complacence.

In 1996, Congress passed legislation whereby law enforcement and emergency response personnel in 120 of the largest cities nationwide were required to undertake training in order to become prepared for the possibility of a terrorist attack. To assist in these preparations, Washington appropriated $30 million in training funds. Yet, according to an April 1998 GAO report, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments,* fewer than a dozen cities had undergone the necessary training. Figures provided by two House members showed that, in fact, 22 cities had completed this training, but in any case, only about one in six of America's major cities was prepared.

According to GAO's report, "While it is not possible to reduce risk to all potential targets against. . .terrorism, risk assessments can help ensure that training, equipment, and other safeguards are justified and implemented based on threat, the vulnerability of the asset to an attack, and the importance of the asset." The Department of Defense (DOD), placed in charged of the preparedness project, questioned the need for risk assessments, which DOD officials claimed would raise implementation costs by as much as $30,000 per city. According to DOD representatives, risk assessments would not affect a city's choice of preparedness equipment.

In December 1998, four months after the Islamic terror network al-Qaeda bombed two U.S. embassies in Africa, U.S. intelligence learned of plans for another attack orchestrated by al Qaeda leader Osama bin Laden. The *New York Times* reported the advisory, but the end of the year passed without incident.

A year later, intelligence sources warned of an attack to occur on December 31, 1999, and although U.S. authorities apprehended suspected al-Qaeda operatives, the story gained little attention in the U.S. media. This time, Americans were more concerned about the apparent Year 2000 problem, or computer glitches associated with the transition from 1999 to 2000.

The Post-September 11, 2001, environment

In April 2002, the Bush administration received what it believed to be credible information concerning a planned suicide bombing on a major U.S. bank. Aside from the threat itself, the White House was faced with the challenge

Explosive materials and electric igniting devices are shown in the car of a suicide bomber just 300 yards from the U.S.Emabssy in Kabul, Afghanistan, where he was stopped by a chance traffic accident in July 2002. AP/WIDE WORLD PHOTOS.

of determining how much to tell the American people so as to keep them properly informed but not spark mass hysteria—and not give away too much information concerning the intelligence resources used in making the threat assessment. Fortunately, the threat passed, but the issue of how to handle suspected threats has not been resolved. When the Office of Homeland Security suggested in February 2003 that Americans purchase duct tape and plastic sheeting to guard their homes against a possible chemical attack, the announcement was greeted with more derision than panic.

The idea of risk assessments dates back to the early Cold War, when intelligence agencies on both sides of the iron curtain were concerned with sizing up one another's relative nuclear and conventional weapons and capabilities. With the end of the Cold War and the rise of international terrorist groups as America's principal foe, risk and threat assessment has become much more challenging. Some experts in the field use the term "net assessment," referring to a complex of factors that includes both the actual threats and the perception of those threats. Integral to such risk assessments, then, is some quantifiable determination of the psychological state both of the terrorists and the threatened population.

FURTHER READING:

BOOKS:

Cameron, Gavin. *Nuclear Terrorism: A Threat Assessment for the 21st Century.* New York: St. Martin's Press, 1999.

Cordesman, Anthony H. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

Haugen, David M. *Biological and Chemical Weapons.* San Diego: Greenhaven Press, 2001.

Roukis, George S., and Hugh Conway. *Global Corporate Intelligence: Opportunities, Technologies, and Threats in the 1990s.* New York: Quorum Books, 1990.

PERIODICALS:

Burns, Jimmy. "Assessing Terror Threat Raises Whitehall Tension." *Financial Times.* (December 14, 2002): 5.

Cummings, Jeanne, and Gary Fields. "Calculating Risks: For Two Tense Days, Bush Team Wrestled with Vague Threat." *Wall Street Journal.* (May 17, 2002): A1.

ELECTRONIC:

Summary/Review of Reports Concerning Threats by Osama Bin Laden. Cornell University Library. <http://www.library.cornell.edu/colldev/mideast/bladen98.htm> (April 7, 2003).

SEE ALSO

HUMINT (Human Intelligence)
Kenya, Bombing of United States Embassy
Terrorism Risk Insurance
Terrorist Threat Integration Center
Vulnerability Assessments

Terrorism, Philosophical and Ideological Origins

ERIC v.d. LUFT

Terrorism is the systematic belief in the political, religious, or ideological efficacy of producing fear by attacking—or threatening to attack—unsuspecting or defenseless populations, usually civilians, and usually by surprise. Terrorist attacks are desperate acts of those who feel themselves to be otherwise powerless. Terrorism is self-righteous, absolutist, and exclusivist. In general, terrorist policy adherents are unwilling or unable to negotiate with their perceived enemies, or prevented by political, social, or economic circumstances from doing so. The philosophical underpinnings of terrorism have become well established worldwide.

The terms "terrorism" and "terrorist" came into the language in the 1790s when British journalists, politicians, orators, and historians used them to describe the Jacobins and other particularly violent French revolutionaries. The terms have evolved since then, and now typically refer to furtive acts by unknown, underground perpetrators, not overt acts by people in power. Nevertheless, some terrorists are secretly harbored, underwritten, trained, or commanded by states that have vested interests against the terrorists' targets. Examples of state-sponsored terrorism include Afghanistan's support of al-Qaeda in 2001, Libya's involvement in the destruction of Pan Am Flight 103 over Lockerbie, Scotland, in 1988, and Adolf Hitler (1889–1945) ordering the Reichstag burned down in 1933 so that he could blame the Communists.

Terrorism as we now understand it was not possible until the invention of gunpowder and subsequent explosives and incendiaries. Before that, small cadres of insignificant conspirators generally lacked the means to achieve sudden massive destruction by stealth. Gunpowder enabled weaklings to outmatch and regularly defeat strong warriors for the first time in history. In a historical sense, modern terrorism began with the unrealized November 5, 1605 "Gunpowder Plot" of Guy Fawkes (1570–1606), who, had he lived in the twelfth century, could not have threatened king and parliament as he did in the seventeenth. But even with the ever-widening proliferation and availability of explosives since then, acts of terrorism remained rare until the middle of the nineteenth century, when anarchism arose as an ideological force.

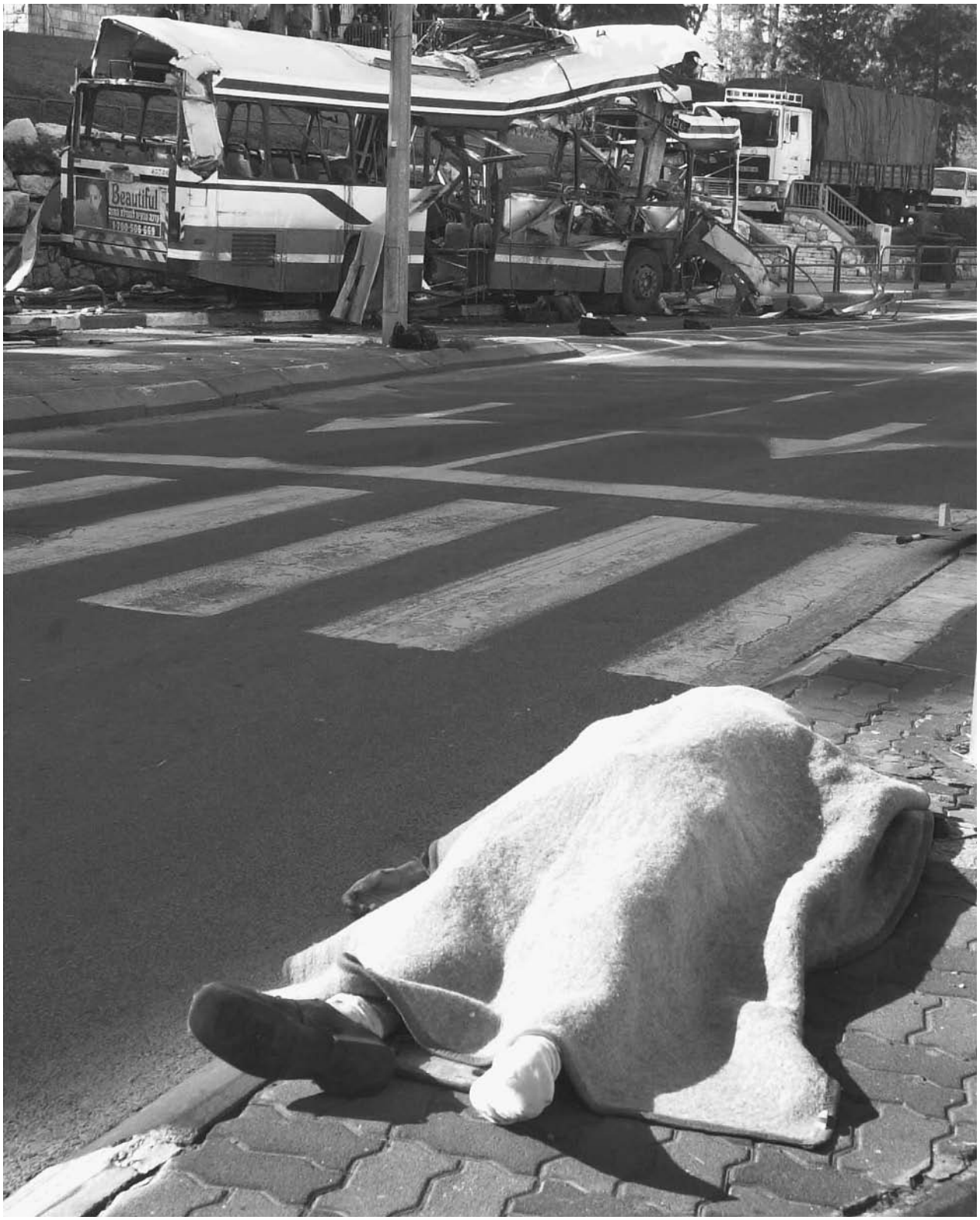
The systematic theory of modern political terrorism arose in Germany during the *Vormä*, i.e., the time between the accession of Prussian King Friedrich Wilhelm IV (1795–1861) in 1840 and the revolutions of 1848. Edgar Bauer (1820–1886) and Mikhail Bakunin (1814–1876), two of the three principal anarchists in the "Young Hegelians," were among terrorism's earliest ideological proponents. The Young Hegelians were a loosely organized group of radical intellectuals influenced to various degrees by the dialectical logic of Georg Wilhelm Friedrich Hegel (1771–1830), the dominant German philosopher of the first half of the nineteenth century. Hegel could not have foreseen that his thought would be perverted in this way and would not have approved of terrorism in any form.

Almost every ideology that became important in the twentieth century arose from the Young Hegelians. These second-generation disciples of Hegel ramified his allegedly self-unifying thought into many disparate movements: socialism and communism came from Karl Marx (1818–1883) and Friedrich Engels (1820–1895), socialism and Zionism from Moses Hess (1812–1875), secular humanism from Ludwig Feuerbach (1804–1872), the "higher criticism" of sacred texts from David Friedrich Strauss (1808–1874) and Bruno Bauer (1809–1882), dialectical historicism from August von Cieszkowski (1814–1894), political liberalism from Arnold Ruge (1802–1880), existentialism and anthropological materialism from Karl Schmidt (1819–1864), individualistic anarchism from Max Stirner (1806–1856), utopian anarchism from Bakunin, and raw anarchism and political terrorism from Edgar Bauer.

In chronological order of their earliest terrorist writings, the first six major theorists of terrorism were Edgar Bauer, Bakunin, Wilhelm Weitling (1808–1871), Karl Heinzen (1809–1880), Sergei Nechaev (1847–1882), and Johann Most (1846–1906).

Edgar Bauer became involved with radical groups in 1839 while a student at the University of Berlin. By 1842 both he and his close friend Engels were members of "The Free Ones" (*Die Freien*), the most notorious club of intellectual agitators in Germany in the early 1840s. His first book, *Bruno Bauer and his Enemies* (1842), defended his brother against government persecution, urged violence, and threatened the Prussian regime with a return to the French Revolution. His 1843 polemic, *Critique's Struggle with Church and State*, advocated terrorism even more blatantly and earned him a prison sentence.

Bakunin, a Russian noble by birth, studied Hegelianism in Russia from 1836 to 1840 and in Berlin from 1841 to



The body of a victim lays covered on the ground at the scene of a bus bomb, background, after a Palestinian suicide bomber detonated nail-studded explosives on the bus in the northern Israeli port city of Haifa in December 2001. AP/WIDE WORLD PHOTOS.

1842. In October 1842, under the pseudonym Jules Elysard, he published "Reaction in Germany," a revolutionary article in Ruge's *Deutsche Jahrbücher*. This essay recommended insurgent violence with lines such as: "The urge to destroy is also a creative urge." Bakunin soon distanced himself from Young Hegelianism, but retained his mutinous attitude toward church and state. His extreme anarchism and nihilism were best expressed in *God and the State*, written in 1871 but published posthumously in 1882.

Weitling was a German tailor who became politically active in 1843. He wrote letters, broadsides, tracts, pamphlets, and books inciting the proletariat to all sorts of violent crimes to free themselves from their oppressors. Even firebrands among the communist, socialist, anarcharist, or syndicalist movements who advocated guerrilla tactics to achieve their political goals were appalled by Weitling's 1843 suggestion that revolutionaries could use arson, theft, and murder to their advantage.

Heinzen is sometimes regarded as the ideological father of modern terrorism, despite the prior writings of Edgar Bauer, Bakunin, and Weitling. Heinzen wrote in 1848 and published in 1849 a powerful essay, "Murder," which claimed that not only the assassinations of leaders, but even the mass murders of innocent civilians, could be effective political tools and should be used without regret. He fled Germany in 1849 and immigrated to America as a "48er," a refugee from the 1848 revolutions. He edited German-language newspapers, notably *Der Pionier*, in several American cities. Although he never specifically recanted his terrorist beliefs, he became a relatively peaceful socialist. He and his wife lived the last twenty years of his life in Roxbury, Massachusetts, as tenants and friends of a prominent early woman physician, Marie Zakrzewska (1829–1902), one of *Der Pionier*'s most ardent supporters.

Nechaev, the son of a former Russian serf, learned early to hate government in general and the czarist regime in particular. As a student at the University of St. Petersburg in 1868, his radical agitations soon forced him into exile. He met Bakunin in Geneva, Switzerland, in March 1869, and became briefly his disciple. They co-wrote several inflammatory pamphlets, including *The Revolutionist's Catechism* (1869), an unrestrained exhortation to antigovernment violence, urging relentless cruelty toward all enemies of the revolution and absolute devotion to the cause of destroying the civilized world. Nechaev returned to Russia in August 1869, murdered a political rival named Ivanov in December 1869, and fled back to Geneva. The Swiss extradited him to Russia in 1872. Convicted of murder in 1873 and sentenced to twenty years of hard labor in Siberia, he died in prison under mysterious circumstances. Fedor Dostoevskii (1821–1881) based his character Pyotr Verkhovensky in *The Possessed* (1871) on Nechaev.

Most was a Social Democrat member of the Reichstag who was forced to flee Germany during Otto von Bismarck's (1815–1898) "Red Scare" of 1878. In exile Most became more radical, relinquished Marxism for anarchism, and edited an inflammatory newspaper, *Die Freiheit*, first in London, briefly in Switzerland, and after 1882 in America. Embittered after serving eighteen months of hard labor in a British prison and after the German Social Democrat Party expelled him *in absentia*, his motto became "Long live hate!" He fell in love with dynamite and spent the rest of his career praising it, learning how to use it, and teaching his fellow revolutionaries how to steal it and the money needed to buy it. He probably invented the letter-bomb, though there is no evidence that he ever used one himself. American agents arrested him for sedition in 1901 because *Die Freiheit* quoted Heinzen's line, "Murder the murderers," the same day that anarchist Leon Czolgosz (1873–1901) killed President William McKinley (1843–1901).

FURTHER READING:

BOOKS:

Breckman, Warren. *Marx, the Young Hegelians, and the Origins of Radical Social Theory: Dethroning the Self.* Cambridge: Cambridge University Press, 1999.

Browning, Gary K. *Hegel and the History of Political Philosophy.* London: Macmillan; New York: St. Martin's, 1999.

Calvert, Peter. "Terror in the Theory of Revolution," *Terrorism, Ideology, and Revolution*, edited by Noel O'Sullivan. Boulder, Colo.: Westview, 1986.

Confronting Fear: A History of Terrorism, edited by Isaac Cronin. New York: Thunder's Mouth, 2002.

Laqueur, Walter. *A History of Terrorism.* New Brunswick, N.J.: Transaction, 2002.

Luft, Eric v.d. "Edgar Bauer and the Origins of the Theory of Terrorism," *The Left-Hegelians: New Philosophical and Political Perspectives*, edited by Douglas Moggach and Andrew Chitty. Albany: SUNY Press, forthcoming.

Mah, Harold. *The End of Philosophy, the Origin of "Ideology": Karl Marx and the Crisis of the Young Hegelians.* Berkeley: University of California Press, 1987.

Marx, Karl, and Friedrich Engels. *The German Ideology*, translated by S. Ryazanskaya. Moscow: Progress, 1964.

———. *The Holy Family, or, Critique of Critical Critique*, translated by R. Dixon. Moscow: Foreign Languages Publishing House, 1956.

Nomad, Max. *Apostles of Revolution.* Boston: Little, Brown, 1939.

Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind, edited by Walter Reich. Baltimore: Johns Hopkins University Press, 1998.

Stirner, Max. *The Ego and His Own*, translated by Steven Byington, revised and edited by David Leopold. Cambridge: Cambridge University Press, 1995.

The Terrorism Reader, edited by David Whittaker. London: Routledge, 2001.

Wittke, Carl Frederick. *The Utopian Communist: A Biography of Wilhelm Weitling, Nineteenth-Century Reformer.* Baton Rouge: Louisiana State University Press, 1950.

SEE ALSO

Terrorism, Intelligence Based Threat and Risk Assessments

Terrorist and Para-State Organizations
Terrorist Organization List, United States

Terrorism Risk Insurance

JUDSON KNIGHT

On November 26, 2002, President George W. Bush signed into law the Terrorism Risk Insurance Act. Intended to cover the private sector in the event of terrorist attacks such as those that occurred on September 11 of the preceding year, the Act provided a system of shared public and private compensation for insured losses resulting from acts of terrorism. The insurance industry was divided in its response to the new legislation, and the high cost of coverage kept away many potential policyholders in the nation's major cities.

On signing the Act, Bush, surrounded by construction workers, announced that "Today we're taking action to strengthen America's economy, to build confidence with America's investors, and to create jobs for America's workers." In recent months, he said, a lack of terrorism insurance had resulted in the delay or cancellation of more than $15 billion in real estate sales.

The new legislation would speed economic recovery in the event of a terrorist attack by providing insurance against such incidents. Not only had such coverage been far from explicitly delineated in many traditional policies, but if a single insurer had to compensate even a fraction of the losses result from an event such as September 11, it could bankrupt the company.

The new law would put in place a temporary federal program to establish such insurance, and rescinded all exclusions to terrorism coverage in existing policy. By backing the new insurance with federal funds, it would also afford the insurance industry an opportunity to stabilize in the new market conditions created by the terrorist attacks. After taking effect on the day it was signed, the law would expire automatically in three years.

The insurance industry was divided in its response, a situation captured by headlines that appeared in two different industry journals over the space of a little more than a week: "TRIA Already Is a Success" (*Business Insurance,* February 24, 2003) and "One-Size-Fits-All TRIA Doesn't Fit" (*National Underwriter,* March 3). The first article, despite its positive spin on the new program, noted that "risk manager response hasn't exactly been overwhelming." One of the problems, noted an industry expert quoted in the second article, was that the law excluded domestic terrorism. Given the sometimes fine line between foreign and domestic terrorists, this could prove problematic.

A report in the *New York Times* that appeared the same day as the *National Underwriter* story noted that corporations in New York City, Washington, D.C., Chicago, and other large cities—areas where terrorist attacks in the future were most likely—had shown little interest in purchasing the new insurance. The reasons were several, including the high cost of premiums, combined with the fact that the federal government would compensate most of the losses in the event of a major terrorist attack.

The article also cited the lack of coverage for an attack by domestic terrorists, a flaw given the fact that prior to September 2001, the worst terrorist attack in American history was perpetrated by Americans—in Oklahoma City on April 19, 1995.

FURTHER READING:

PERIODICALS:

Bumiller, Elisabeth. "Government to Cover Most Costs of Insurance Losses in Terrorism." *New York Times* (November 27, 2002): A1.

Bush, George W. "Remarks on Signing the Terrorism Risk Insurance Act of 2002." *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2096–97.

Hays, Daniel. "One-Size-Fits-All Doesn't Fit: Study." *National Underwriter* 107, no. 9 (March 3, 2003): 26.

Romano, Jay. "Terrorism Insurance, at a Price." *New York Times* (March 9, 2003): 5.

Treaster, Joseph B. "Insurance for Terrorism Still a Rarity." *New York Times* (March 8, 2003): C1.

"TRIA Already Is a Success." *Business Insurance* 37, no. 8 (February 24, 2003): 8.

ELECTRONIC:

Terrorism Risk Insurance Program. U.S. Department of the Treasury. <http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/> (March 28, 2003).

SEE ALSO

September 11 Terrorist Attacks on the United States
Terrorism, Intelligence Based Threat and Risk Assessments
Treasury Department, United States

Terrorist and Para-State Organizations

Para-state organizations challenge some aspect of the authority of recognized governments or states. Many para-state groups, illegal within their own country or territory, seek international recognition at the Unrepresented Nations and Peoples Organization (UNPO), a non-governmental organization headquartered in The Hague.

Members of the Laskar Mujahidin listen to a briefing from their leader in Solo, Central Java, Indonesia, in October 2002, the same year that Washington branded the Islamist extremist group a terrorist organization. AP/WIDE WORLD PHOTOS.

There are no clear defining lines between guerilla forces and para-state organizations. Guerilla warfare refers to more organized, widespread, or formal armed resistance by paramilitary or para-state groups (usually wearing some sort of insignia or uniform) toward an occupying force. In many areas of the world, guerilla warfare tactics are used by paramilitary groups against government forces.

Moreover, history is replete with causes and movements, initially branded as "illegitimate" or "para-state" organizations that ultimately become the ruling government (i.e., transforming the group from a "para-state" to the state itself). In some cases, an organization branded "terrorist" or "outlaw" by the ruling government may be considered a legitimate political movement or a group of "fighters" for a cause embraced by a segment of the population.

For example, the African National Congress—once headed by Nobel Laureate Nelson Mandela—was for decades branded a terrorist and outlaw group by the now abolished apartheid South African government.

In general, it is the commission of acts of violence that brand organizations as para-state terrorist groups as opposed to legitimate political parties or national liberation movements that do not engage in violence or armed struggle in an attempt to change governments.

The definition of terrorist is, however, not entirely subjective. Under United States law, terrorist activity is so labeled by "any activity which is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following: The highjacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle); The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained; A violent attack upon an internationally protected person (defined in section 1116(b)(4) of title 18, United States Code) or upon the liberty of such a person; or an assassination."

MGA KIDNAPPER!
MGA MAMAMATAY-TAO!

Abu Sabaya

Hamsiraji Sali

Khadafi Janjalani

Abu Solaiman

Isnilon Hapilon

PREMYO PARA SA IMPORMASYON
HANGGAN $5,000,000

The U.S. Government is offering a reward of up to $5,000,000 for information leading to the arrest or conviction of the terrorists responsible for the kidnapping of Martin and Gracia Burnham, and the kidnapping and murder of Guillermo Sobero. If you have any information about any individuals committing acts of international terrorism against U.S. persons or property, please contact the U.S. Embassy.

PREMYO PARA SA KATARUNGAN

www.rewardsforjustice.net

1-800-10-739-2737 (MANILA) 1-800-877-3927 (USA)

Kung Cell phone ang gagamitin ay tumawag lamang sa 02-526-9832/9833/9834

LAHAT NG IMPORMASYON NA MATATANGAP NAMIN AY ITUTURING SIKRETO

A handout circulated by the U.S. embassy in Manila after announcing the U.S. government's offer of a $5 million reward in May 2000, for the capture of leaders of the Abu Sayyaf Islamist extremist group that kidnaped two Americans and killed another on Basilan Island, southern Philippines. AP/WIDE WORLD PHOTOS.

U.S. law and statutes also define as acts of terrorism "the use of any biological agent, chemical agent, or nuclear weapon or device; or explosive, firearm, or other weapon or dangerous device. . . with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property."

State-sponsored terrorism. In addition to para-state organizations that usually operate within defined borders, a state itself can also act to sponsor terrorism or terrorist organizations.

As of April 1, 2003, the U.S. State Department had designated the following countries state sponsors of international terrorism: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. The State Department asserts that although ". . . most no longer engage directly in terrorist activity, they may support terrorist groups by providing funding or arms."

Terrorist organizations. Annually, the U.S. Department of State publishes a list of designated foreign terrorist organizations (FTOs). In 2002, the State Department designated 33 groups as FTOs. The State Department's formal list focuses on groups who have recently engaged in terrorist attacks or are otherwise highly active. In addition, the State Department's annual report to Congress, *Patterns of Global Terrorism*, also identifies and profiles organizations that in the past have been designated as terrorist organizations.

Organizations not formally designated as foreign terrorist groups, but listed as terrorist organizations in the 2001 report to Congress include the following organizations: Alex Boncayao Brigade (ABB); Al-Ittihad al-Islami (AIAI); Allied Democratic Forces (ADF); Anti-Imperialist Territorial Nuclei (NTA); Army for the Liberation of Rwanda (ALIR); Cambodian Freedom Fighters (CFF); Continuity Irish Republican Army (CIRA); First of October Antifacist Resistance Group (GRAPO); Harakat ul-Jihad-I-Islami (HUJI); Harakat ul-Jihad-I-Islami/Bangladesh (HUJI-B); Islamic Army of Aden (IAA); Irish Republican Army (IRA); Al Jama'a al-Islamiyyah al-Muqatilah bi-Libya; Japanese Red Army (JRA); Jemaah Islamiya (JI); Kumpulan Mujahidin Malaysia (KMM); Lord's Resistance Army (LRA); Loyalist Volunteer Force (LVF); New People's Army (NPA); Orange Volunteers (OV); People Against Gangersterism and Drugs (PAGAD); Red Hand Defenders (RHD); Revolutionary Proletarian Initiative Nuclei (NIPR); Revolutionary United Front (RUF); The Tunisian Combatant Group (TCG); Tupac Amaru Revolutionary Movement (MRTA); Turkish Hizballah; and the Ulster Defense Association/Ulster Freedom Fighters (UDA/UVF).

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the record briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Terrorist Organization List, United States

The United States Secretary of State formally designates "Foreign Terrorist Organizations" (FTO) that threaten United States interests. Within the Department of State, the Office of the Coordinator for Counterterrorism is assigned the primary responsibility for monitoring available intelligence and public news accounts of terrorist activities so that they may advise the Secretary on decisions related to terrorism-related designations. The designation process, in part, focuses on groups who have recently engaged in terrorist attacks.

Although designations can be modified at any time (i.e., groups can be added or deleted from the list by the Secretary of State) designations normally expire in two years unless renewed. Changes in the list require a formal notification of Congress. Organizations have the right under U.S. law—should they choose to appear—of appealing an FTO designation to United States Court of Appeals for the District of Columbia Circuit within 30 days of such designation.

Impact of FTO designation. When an organization is designated as an FTO it becomes unlawful for a person in the United States (or U.S. jurisdictions) to knowingly provide "material support or resources" (e.g. money, aid, advice, training, etc.) to a designated FTO.

FTO members may not legally enter the U.S. or its territories, and may be deported upon discovery.

U.S. banks or other financial institutions that control accounts in which agents of FTOs have some interest must report account existence and activities to the Office

of Foreign Assets Control of the U.S. Department of the Treasury.

Designated FTOs. The U.S. Department of State publishes a list of designated foreign terrorist organizations as a part of its report, *Patterns of Global Terrorism*, submitted annually to Congress.

Groups designated as foreign terrorist organizations by the U.S. Department of State, as of January 30, 2003, include the following organizations: "Abu Nidal Organization (ANO); Abu Sayyaf Group; Al-Aqsa Martyrs Brigade; Armed Islamic Group (GIA); Asbat al-Ansar; Aum Shinrikyo; Basque Fatherland and Liberty (ETA); Communist Party of the Philippines/New People's Army (CPP/NPA); Gama'a al-Islamiyya (Islamic Group); HAMAS (Islamic Resistance Movement); Harakat ul-Mujahidin (HUM); Hizballah (Party of God); Islamic Movement of Uzbekistan (IMU); Jaish-e-Mohammed (JEM) (Army of Mohammed); Jemaah Islamiya organization (JI) al-Jihad (Egyptian Islamic Jihad); Kahane Chai (Kach); Kurdistan Workers' Party (PKK); Lashkar-e Tayyiba (LT) (Army of the Righteous); Liberation Tigers of Tamil Eelam (LTTE); Mujahedin-e Khalq Organization (MEK); National Liberation Army (ELN); Palestine Liberation Front (PLF); Palestinian Islamic Jihad (PIJ); PFLP-General Command (PFLP-GC); Popular Front for the Liberation of Palestine (PFLP); al-Qaeda; Real IRA; Revolutionary Armed Forces of Colombia (FARC); Revolutionary Nuclei (formerly ELA); Revolutionary Organization 17 November; Revolutionary People's Liberation Army/Front (DHKP/C); Salafist Group for Call and Combat (GSPC); Shining Path (Sendero Luminoso, SL); United Self-Defense Forces of Colombia (AUC)."

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing." May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Guerilla Warfare
Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organizations, Freezing of Assets

Terrorist Organizations, Freezing of Assets

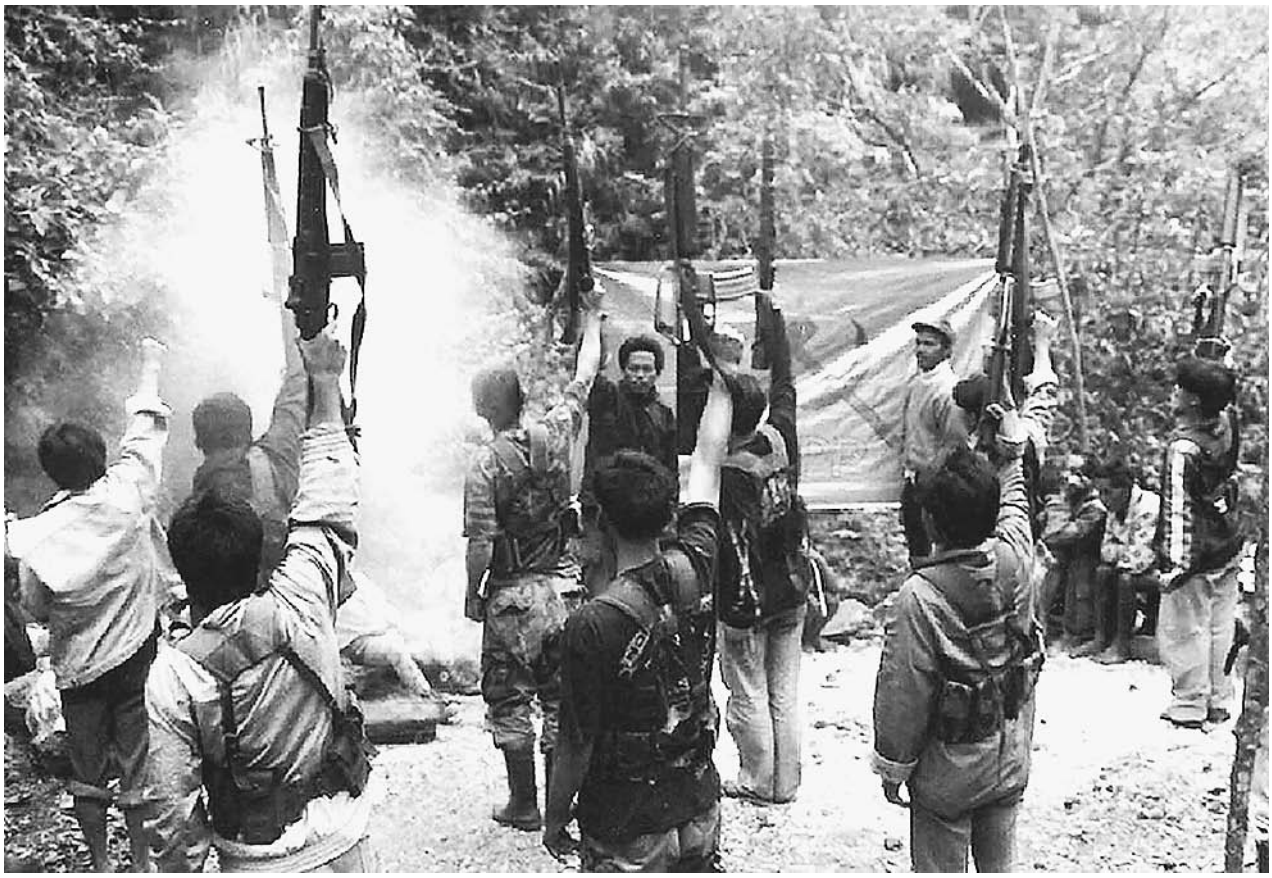
■ MARTIN J. MANNING

Monitoring the frozen assets of terrorist organizations is something that took on a new focus and urgency after the events of September 11, 2001. The United States and its allies have arrested about 2,290 suspected terrorists and terrorist financiers in 99 countries, designated about 250 individuals and organizations as terrorists or terrorist supporters, and seized more than $113 million in assets since the terrorist attacks of September 11, 2001.

On September 24, 2001, President George W. Bush stated, "We will direct every resource at our command to win the war against terrorists, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence. We will starve the terrorists of funding." The president directed the federal government to wage the nation's war against the financing of global terrorism, and we have continued to devote our resources and extensive expertise to fulfill this mandate. In actions and in words, the Treasury Department has shown that in the war against terrorism, financial intermediaries and facilitators who infuse terrorist organizations with money, materiel, and support will be held accountable along with those who perpetrate terrorist acts.

Immediately after the terrorist attacks, Congress worked closely with the Department of the Treasury, along with the Department of Justice and other agencies and departments, to make significant improvements in the law that enhances Treasury's ability to tackle the issue of terrorist financing in a more unified, cohesive and aggressive manner. Of particular importance to the counter-terrorist efforts, the U.S. Patriot Act, enacted into law on October 26, 2001, expanded the law enforcement and intelligence community's ability to access and share critical financial information regarding terrorist investigations. In the months immediately following the September 11 attacks, the Department of the Treasury took six principal steps to identify and pursue financial underwriters of terrorism:

- worked with other U.S. Government agencies to implement Executive Order 13224;
- established Operation Green Quest, an inter-agency task force, to target financial networks and mechanisms;
- won the adoption of UN Security Council Resolutions 1373 and 1390 which require member nations to disrupt terrorist financing;
- engaged other multilateral institutions such as the Financial Action Task Force (FATF) and the international financial institutions to focus on terrorist financing;



New People's Army guerrillas, the armed wing of the Communist Party of the Philippines (CPP), photographed at a clandestine assembly in the Cordillera region in northern Philippines, 2002. ©AFP/CORBIS.

- implemented the U.S. Patriot Act provisions to broaden and deepen access to critical financial information in the war against terrorist financing and to expand the anti-money laundering regulatory network;
- shared information across the federal government, with the private sector and among U.S. allies to crack down on terrorist financiers.

For the first time, the 2002 National Money Laundering Strategy (NMLS) contained such a strategy, with a discrete set of objectives and priorities targeting terrorist financing. Goal Two of the NMLS identified financial mechanisms or systems by which terrorist funding was initiated and sought to attack these mechanisms on an interagency and coordinated basis. The NMLS stated that terrorist groups tap into a wide range of sources for their financial support, including otherwise legitimate enterprises, such as construction companies, honey shops, tanneries, banks, agricultural commodities growers and brokers, trade businesses, bakeries, restaurants, and bookstores. The strategy focused on the following areas:

- targeted intelligence gathering;
- freezing of suspect assets;
- law enforcement actions;
- diplomatic efforts and outreach;
- smarter regulatory scrutiny;
- outreach to the financial sector; and
- capacity building for other governments and the financial sector through Treasury and other departmental technical assistance programs.

The NMLS is an integrated inter-agency strategy that draws on the expertise and resources of the Treasury Department, the Department of Justice, the Department of State and other departments and agencies of the federal government, as well as on foreign partners and on the private sector. Its mission is to first, identify appropriate financial targets through technology, intelligence, investigative resources, and regulations to locate and freeze the assets of terrorists, wherever they may be located.

Second, the NMLS freezes terrorist-related assets on a global scale. The U.S. government has frozen over U.S. $35 million in terrorist-related assets since September 11, 2001, and the international community has frozen an additional U.S. $78 million. More important than the dollars frozen is the dismantling of these financial pipelines, which served to transmit far greater sums of money for terrorist purposes. Third, the NMLS coordinates effective

law enforcement actions, both domestically and internationally, against terrorist cells and networks. Internationally, Treasury has deployed Customs attachés and representatives from Treasury's Office of Foreign Assets Control (OFAC) in strategic embassies around the world to facilitate cooperation with host countries and regions in combating terrorist financing. Between September 12, 2001, and October 28, 2002, international law enforcement cooperation has led to approximately 2290 arrests of suspected terrorists and their financiers in 99 countries.

Fourth, together with other agencies, the NMLS uses existing diplomatic resources and regional and multilateral engagements to ensure international cooperation, collaboration and capability in dismantling terrorist financing networks. One of the bilateral initiatives is the U.S. Government's designation of Foreign Terrorist Organizations (FTOs). Under authorities provided by the Antiterrorism and Effective Death Penalty Act of 1996, the Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, has designated 35 groups as foreign terrorist organizations. The designations make it a criminal offense for American persons to knowingly provide funds or other forms of material support for these designated groups. Some other countries have used the designations as a guideline for their own efforts to curb terrorism financing.

Fifth, the NMLS implements smarter regulatory scrutiny by training the financial sectors to concentrate enhanced due diligence and suspicious activity monitoring on terrorist financing and money laundering typologies. Through the U.S. Patriot Act authorities, Treasury has been able to expand regulatory scrutiny to all businesses within the financial sector that may be susceptible to terrorist or criminal abuse. Sixth, the NMLS regulates expansion under the authorities of the Patriot Act in full consultation with the private financial sectors.

On October 1, 2002, FinCEN's (Financial Crimes Enforcement Network) secure link with financial institutions, the Patriot Act Communications System (PACS), became operational along with several capacity-building initiatives with other governments and the private sector with respect to terrorist financing. For example, Treasury is co-chairing a FATF Working Group on Terrorist Financing, which, among other issues, is charged with identifying technical assistance needs of various governments around the world. This Working Group is collaborating with donor states, the International Monetary Fund, the World Bank, and the UN Counter-Terrorism Committee in coordinating the delivery of technical assistance to those governments.

Actions Taken Against Terrorist Financing

The most visible and immediately effective tactic of U.S. terrorist financing strategy has been designating and blocking the accounts of terrorists and those associated with financing terrorist activity. Publicly designating terrorists, terrorist supporters and facilitators, and blocking their ability to receive and move funds through the world's financial system has been and is a crucial component in the fight against terrorism. On September 24, 2001, President Bush issued Executive Order 13244, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism."

The Department of the Treasury's Office of Enforcement, in conjunction with Treasury's Office of International Affairs and the Office of Foreign Assets Control, has helped lead U.S. efforts to identify and block the assets of terrorist-related individuals and entities within the United States and worldwide. Currently, 250 individuals and entities are publicly designated as terrorists or terrorist supporters by the United States, and since September 11th, over $113 million in assets of terrorists has been frozen around the world. Beyond simply freezing assets, these U.S. and international actions to publicly identify terrorists and their supporters advance global interests in terrorist financing and combating terrorism by:

- shutting down the pipeline by which designated parties moved money and operated financially in the mainstream financial sectors;
- informing third parties who may be unwittingly financing terrorist activity of their association with supporters of terrorism;
- providing leverage over those parties not designated who might otherwise be willing to finance terrorist activity;
- exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers;
- forcing terrorists to use alternative and potentially more costly informal means of financing their activities; and
- supporting diplomatic effort to strengthen other countries' capacities to combat terrorist financing through the adoption and implementation of legislation that allows states to comply with their obligations under UN Security Council Resolutions 1390 and 1373.

Currently, over 165 countries and jurisdictions have blocking orders in force. Alternative financial mechanisms to combat terrorist financing conducted through these mechanisms include the following measures.

Protecting charities from terrorist abuse. Under the authority of E.O. [Executive Order] 13224, the United States has designated twelve charitable organizations as having ties to al-Qaeda or other terrorist groups. In addition, the United States has designated and blocked the assets of the largest U.S.-based Islamic charity, which acted as a funding vehicle for the HAMAS terrorist organization.

The FATF Special Recommendation VIII on Terrorist Financing commits all member nations to ensure that nonprofit organizations cannot be misused by financiers of

terrorism. The United States is co-chairing the FATF Terrorist Financing Working Group that has recently produced an international best practices paper on how to protect charities from abuse or infiltration by terrorists and their supporters.

Efforts are underway to assist U.S.-based charities concerned that their distribution of funds abroad might reach terrorist-related entities and trigger a blocking action on the part of the Treasury Department—the Department has developed voluntary best practices guidelines for all U.S.-based charities. The Treasury Department developed these guidelines in response to requests from the Arab American and American Muslim communities, who reported a reduction in charitable giving and an increased apprehension among donors as a consequence of the Treasury Department's blocking of the three domestic charities.

Regulating *Hawalas*: informal value transfer systems. Terrorists have also used *Hawalas* and other informal value transfer systems as a means of terrorist financing. The word "hawala" (meaning "trust") refers to a fast and cost-effective method for the worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector. In some nations, *Hawalas* are illegal; in others they are active but unregulated. It is, therefore, difficult to measure accurately the total volume of financial activity associated with the system; however, it is estimated that, at a minimum, tens of billions of dollars flow through *Hawalas* and other informal value transfer systems on an annual basis.

The United States has already taken steps to regulate *Hawalas* and informal value transfer systems. The U.S. Patriot Act requires money remitters (informal or otherwise) to register as "money services business" or "MSBs," thereby subjecting them to existing money laundering and terrorist financing regulations, including the requirement to file Suspicious Activity Reports (SARs). As a result, well over 11,000 money service businesses have registered with the federal government and are now required to report suspicious activities. The Act makes it a crime for the money transfer business owner to move funds that he knows are the proceeds of a crime or are intended to be used in unlawful activity. Failure by money service business principals to register with FinCEN and/or failure to obtain a state license also are federal crimes.

FATF Special Recommendation VI addresses this issue by demanding that countries register or license informal value transfer businesses and subject them to all of the FATF Recommendations that applies to banks and non-bank financial institutions. In addition, at a conference on hawala in the United Arab Emirates (UAE) in May, 2002, a number of governments agreed to adopt FATF Special Recommendation VI and shortly thereafter, the UAE government announced it would impose a licensing requirement on hawala operators operating within its borders. Participants at the UAE meeting drafted and agreed upon the Abu Dhabi Declaration on Hawala, which set forth a number of principles calling for the regulation of *Hawalas*.

Combating bulk cash smuggling. Bulk cash smuggling has proven to be yet another means of financing adopted by terrorists and their financiers. Customs has executed 650 bulk cash seizures totaling $21 million, including $12.9 million with a Middle East connection. Pursuing bulk cash smuggling from a domestic perspective, however, is not enough; disruption of this tactic requires a global approach.

Investigating trade-based terrorist financing. With respect to trade-based financial systems, authorized enforcement agencies continue to investigate the use of licit and illicit international trade commodities, for example, diamonds, gold, honey, and cigarettes, as well as narcotics, to fund terrorism. The U.S. Customs Service has developed a state-of-the-art database system to identify anomalous trade patterns for imports and exports to and from the United States. In the past, Customs has demonstrated this system to other nations, including Colombia, with excellent results.

Investigating terrorist cyber-fundraising activities. Terrorist groups now exploit the Internet to recruit supporters and raise terrorist funds. Developing a strategy to counter such cyber-fundraising activities is a responsibility that the Treasury Department assumed in its 2002 Anti-Money Laundering Strategy.

Operation "Green Quest." On October 25, 2001, Treasury created Operation Green Quest (OGQ) to focus the Treasury Department's financial expertise in the war against terrorist financing. OGQ identifies and attacks terrorist financing through a systemic financial approach. OGQ specializes in identifying financial mechanisms, such as illegal money remitters, and searching those systems to identify potential terrorist financing.

OGQ is led by the United States Customs Service, and includes the Internal Revenue Service, the Secret Service, the Bureau of Alcohol Tobacco and Firearms (ATF), Treasury's Office of Foreign Assets Control (OFAC), FinCEN, the Postal Inspection Service, the Federal Bureau of Investigation (FBI), and the Department of Justice. The financial expertise of the Treasury Bureaus, along with the exceptional experience of our partner agencies and departments, is also utilized in this operational attack on terrorist financing.

International Efforts

Internationally, the United States has worked not only through the United Nations on blocking efforts, but also through multi-lateral organizations and on a bi-lateral

basis to promote international standards and protocols for combating terrorist financing. The Treasury Department has continuously engaged the international community in developing and strengthening counter-terrorist financing initiatives and regimes.

The United Nations 1267 Committee is responsible for UN designations of individuals and entities associated with al Qaeda, Osama bin Laden, and the Taliban. States wishing to propose a name for UN designation typically include a statement of the basis for designation, along with identifying information for the use of financial institutions, customs and immigration officials, and others who must implement sanctions. If no state objects to the proposed designation within 48 hours after a name is circulated by the Committee Chairman, the designation becomes effective. The 1267 Committee then puts out an announcement on its web site and all UN member states are required to freeze any assets held by the designated party(ies), without delays.

Financial Action Task Force (FATF). Since 1989, the 31-member FATF has served as the preeminent anti-money laundering multilateral organization in the world. The United States has played a leading role in the development of this organization. Capitalizing on this financial crime expertise, on October 31, 2001, at the United States' initiative, the FATF issued Eight Special Recommendations on terrorist financing, requiring all member nations to:

- Ratify the UN International Convention for the Suppression of the Financing of Terrorism and implement relevant UN Resolutions against terrorist financing;
- Criminalize the financing of terrorism, terrorist acts and terrorist organizations;
- Freeze and confiscate terrorist assets;
- Require financial institutions to report suspicious transactions linked to terrorism;
- Provide the widest possible assistance to other countries' laws enforcement and regulatory authorities for terrorist financing investigations;
- Impose anti-money laundering requirements on alternative remittance systems;
- Require financial institutions to include accurate and meaningful originator information in money transfers; and
- Ensure that non-profit organizations cannot be misused to finance terrorism.

Many non-FATF counties have committed to complying with the Eight Recommendations and over 90 non-FATF members have already submitted self-assessment questionnaires to FATF describing their compliance with these recommendations. Together with the Departments of State and Justice, Treasury will continue to work with the FATF to build on its successful record in persuading jurisdictions to adopt anti-money laundering and anti-terrorist financing regimes to strengthen global protection against terrorist finance.

As part of this effort, FATF has established a Working Group on Terrorist Financing (Working Group), which the United States is co-chairing with Spain, devoted specifically to developing and strengthening FATF's efforts in this field. At the most recent FATF Plenary in October, 2002, the Working Group, in collaboration with the World Bank, the International Monetary Fund, and the UN, identified a number of countries to receive priority technical assistance in order for them to come into compliance with the Eight Special Recommendations on Terrorist Financing.

Egmont Group. The Egmont Group represents 69 Financial Intelligence Units (FIUs) from various countries around the world. FinCEN is the FIU for the United States. The FIU in each nation receives financial information (such as SARs) from financial institutions pursuant to each government's particular anti-money laundering laws, analyzes and processes these disclosures, and disseminates the information domestically to appropriate government authorities and internationally to other FIUs in support of national and international law enforcement operations.

Successful results. International law enforcement cooperation has resulted in approximately 2290 arrests of suspected terrorists and their financiers in 99 countries from September 12, 2001 through October 28, 2002. Some of these arrests have led to the prevention of terrorist attacks in Singapore, Morocco and Germany, and have uncovered al-Qaeda cells and support networks in Italy, Germany, Spain, the Philippines and Malaysia, among other places. In addition, soon after September 11th, a Caribbean ally provided critical financial information through its FIU to FinCEN that allowed the revelation of a financial network that supported terrorist groups and stretched around the world.

On September 24, 2001, President Bush implemented Executive Order 13224 which expands the U.S. government's power and authority to target terrorist organizations to freeze and block their assets. In that same period, the United Nations adopted UN Security Council resolutions 1373 and 1390, directing member states to criminalize terrorist financing and adopt regulatory regimes to detect and deter terrorist financing. On August 29, 2002, the Office of Foreign Assets Control established the Specially Designated Nationals (SDN) and Blocked Persons List, which is updated as groups and individuals are added or removed. Most recently, in March 2003, the U.S. Department of the Treasury created a new unit to set strategy and policy for combating terrorist financing. The new Executive Office for Terrorist Financing and Financial Crimes would work with the financial services industry to locate terror-related accounts and groups. It will also oversee Treasury's Financial Crimes Enforcement Network

(FINCen), an investigative and information-gathering bureau, and the Office of Foreign Asset Controls (OFAC), which carries out U.S. orders blocking bank accounts and freezing assets of suspected terrorist groups and their supporters.

In order to continue Treasury's leadership on these critical issues, the new Office is charged with developing and implementing U.S. government strategies to combat terrorist financing domestically and internationally (in concert with Treasury's International Affairs Task Force on Terrorist Financing); developing and implementing the National Money Laundering Strategy, as well as other policies and programs to fight financial crimes; participating in the department's development and implementation of U.S. government policies and regulations in support of the Patriot Act, including outreach to the private sector; joining in representation of the United States at focused international bodies dedicated to fighting terrorist financing and financial crimes; and developing U.S. government policies relating to financial crimes.

FURTHER READING:

BOOKS:

Blunden, Bob. *The Money Launderers: How They Do It, and How to Catch Them at It.* Chalford, England: Management Books, 2001.

Doyle, Charles. *The USA PATRIOT Act: A Legal Analysis.* Washington, D.C.: Congressional Research Service, Library of Congress, 2002.

Lilley, Peter. *Dirty Dealing: The Untold Truth about Global Money Laundering.* London: Kogan Page, 2000.

Naylor, R. T. *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy.* Ithaca, NY: Cornell University, 2002.

Savla, Sandeep. *Money Laundering and Financial Intermediaries.* The Hague and Boston: Kluwer Law International, 2001.

U.S. Congress. House Committee on Financial Services."Dismantling the Financial Infrastructure of Global Terrorism." Hearing, 107th Congress, 1st Session, Washington, D.C.: Government Printing Office, 2001.

———. House Committee on Financial Services. Subcommittee on Oversight and Investigations. "ATRIOT Act Oversight: Investigating Patterns of Terrorist Financing."Hearing, 107 Congress, 2nd session, February 12, 2002. Washington, D.C.: Government Printing Office, 2002.

U.S. Department of the Treasury. Financial Crimes Enforcement Network. "U.S. Compendium of Selected Anti-Money Laundering Statutes and Rules." Vienna, VA: 1997.

PERIODICALS:

Morais, Herbert V. "The War against Money Laundering, Terrorism, and the Financing of Terrorism," *Lawasia Journal* (2002): 1–32.

Serino, Robert B. "Money Laundering, Terrorism, and Fraud." *ABA Bank Compliance* (March/April 2002): 23–26.

Shams, Heba. "Using Money Laundering Control to Fight Corruption: An Extraterritorial Instrument." *International Financial and Economic Law* no. 27, 2000).

ELECTRONIC:

International Monetary Fund. "Enhancing Contributions to Combating Money Laundering: Policy Paper." <http://www.imf.org/external/np/ml/2001/eng/042601.htm> (April; 14, 2003).

International Monetary Fund. Financial System Abuse, Financial Crime and Money Laundering: Background Paper. <http://www.imf.org/external/np/ml/2001/eng/021201.htm> (April 14, 2003).

U.S. Treasury Department. "High Intensity Money Laundering and Related Financial Crimes Areas (HIFCAs) Designations" <www.ustreas.gov/fincen/hifcadesignations.html> (April 14, 2003).

U.S. Treasury Department, Office of Foreign Assets Control. "Specially Designated Nationals and Blocked Persons." <http://www.ustreas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf> (April 14, 2003).

SEE ALSO

IMF (International Monetary Fund)
Intelligence and International Law
Intelligence and Law Enforcement Agencies
Intelligence Authorization Acts, United States Congress
Intelligence Community
Intelligence Officer
Intelligence Policy and Review (OIPR), United States Office
Intelligence Support, United States Office
Secret Service, United States
Terror Alert System, United States
Terrorism, Intelligence Based Threat and Risk Assessments
Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Threat Integration Center
United States, Intelligence and Security

Terrorist Threat Integration Center

CARYN E. NEUMANN

The Terrorist Threat Integration Center (TTIC) improves the ability of the United States to thwart terrorist attacks by analyzing and sharing intelligence emanating from anywhere in the world. Opened in May 2003, as part of President George W. Bush's initiative to revamp counterterrorism intelligence, the goal of the TTIC is to provide a comprehensive threat picture. While it operates under the direction of the Central Intelligence Agency chief, TTIC is staffed by counterterrorism experts from the CIA, Federal Bureau of Investigation (FBI) and the Departments of Defense and Homeland Security. It will eventually serve as the hub of all counterterrorism analysis.

In the wake of the 2001 World Trade Center attack, the intelligence gathering agencies in the United States came under heavy criticism from Congress and the public for their failure to predict and halt the terrorist assault. Government inquiries concluded that a lack of information sharing prevented anyone from doing sufficient analysis and taking action. The FBI, as the preeminent domestic intelligence agency, received the bulk of the blame. In response to these intelligence shortcomings, Bush established the TTIC and thereby ended the FBI's decades-long reign as the nation's chief provider of domestic intelligence.

The aim of the TTIC is to seamlessly unite intelligence from a variety of sources to assist executive branch policymaking decisions. To this end, TTIC has unfettered access to all terrorist threat intelligence from raw reports to finished analytic assessments. The analysts in the center measure the reliability of information from interrogated al-Qaeda prisoners, study warnings from foreign law-enforcement and spy agencies, assess tips from informants, examine satellite photos, and read transcripts of wiretapped conversations. No TTIC staff members conduct intelligence collection operations.

TTIC plays the lead role in creating a national counterterrorism structure to share across agency lines all terrorist threat intelligence, whether gathered in the U.S. or overseas. The tasking system of TTIC will be implemented in three phases. In its initial phase, the TTIC provides integrated terrorist threat analysis for the senior national leadership. The center's duties will include compiling the "daily threat matrix" that is instrumental to the president's decisions in the war on terror. In its secondary phase, TTIC will be the principal gateway for policymaker requests for analysis of potential terrorist threats to U.S. interests and will maintain a database of known and suspected terrorists that can be accessed by government officials at all levels who possess the appropriate security clearance. In its tertiary and final stage, TTIC will serve as the U.S. government hub for all terrorist threat-related analytic work.

As the TTIC is a joint venture of participating agencies, the Director of Central Intelligence, as statutory head of the U.S. intelligence community, oversees its activities. The head of the TTIC is selected by CIA chief in consultation with the Director of the FBI, the Attorney General, and the Secretaries of Homeland Security and Defense. At the initial stage, total staffing of TTIC is 60 U.S. government employees plus additional contractors. In the second phase of implementation, employment will rise to 120 people. In the final stage, TTIC will have a staff level of 250 to 300 employees. TTIC is scheduled to be located in a facility with the FBI Counterterrorism Division and the CIA Counterterrorist Center. This co-location is expected to enhance information sharing and maximize counterterrorism resources while reducing redundant capabilities.

The terrorist attack of September 11, 2001 made apparent the need to change the intelligence gathering strategy of the United States. While most government leaders and members of the public have applauded the goal of fusing intelligence analysis from the FBI and CIA, data reflecting the efficiency of the TTIC to close intelligence gaps while safeguarding individual liberties will take months or years to accumulate.

FURTHER READING:

ELECTRONIC:

United States Department of State, International Information Programs. "Fact Sheet: New Terrorist Integration Center Will Open May 1. February 14, 2003 <http://usinfo.state.gov/topical/pol/terror/03021404.htm> (February 25, 2002).

SEE ALSO

Bush Administration (2001–), United States National Security Policy
CIA (United States Central Intelligence Agency)
United States, Counter-Terrorism Policy
DCI (Director of the Central Intelligence Agency)
DoD (United States Department of Defense)
FBI (United States Federal Bureau of Investigation)
Homeland Security, United States Department
World Trade Center, 2001 Terrorist Attack

Thermal Body Scanners.

SEE *Communicable Diseases, Isolation, and Quarantine.*

Thin Layer Chromatography

BRIAN HOYLE

Thin layer chromatography, which is typically abbreviated as TLC, is a type of liquid chromatography that can separate chemical compounds of differing structure based on the rate at which they move through a support under defined conditions.

TLC is useful in detecting chemicals of security concern, including chemical weapons, explosives, stabilizing chemicals for rocket propellants, and illicit drugs. For example, the Forensic Service Center of Lawrence Livermore National Laboratory has designed a computerized and portable TLC machine that can be taken to the field, and which has the ability to analyze 20 samples at a time. Analysis can be completed within 30 minutes.

TLC as it is still practiced today was introduced by Justus Kirchner in 1951. From its beginning, the technique was an inexpensive, reliable, fast, and easy to perform means of distinguishing different compounds from each other. The method was qualitative—it showed the presence of a compound but not how much of the compound

was present. In the late 1960s, TLC was refined so that it could reliably measure the amounts of compounds. In other words, the technique became quantitative. Further refinement reduced the thickness of the support material and increased the amount of the separating material that could be packed into the support. In High Performance TLC (HPTLC) the resolution of chemically similar compounds is better than with conventional TLC, and less sample is required. HPTLC requires specialized analysis equipment, and so is still not as popular or widespread as conventional TLC.

In TLC a solution of the sample is added to a layer of support material (i.e., grains of silica or alumina) that has been spread out and dried on a sheet of material such as glass. The support is known as the plate. The sample is added as a spot at one end of the plate. The plate is then put into a sealed chamber that contains a shallow pool of chemicals (the solvent), which is just enough to wet the bottom of the plate. As the solvent moves up through the plate support layer by capillary action, the sample is dragged along. The different chemical constituents of the sample do not move at the same speed, however, and will become physically separated from one another. The positions of the various sample constituents and their chemical identities are determined by physical methods (i.e., ultraviolet light) or by the addition of other chemical sprays that react with the sample constituents.

FURTHER READING:

BOOKS:

Fried, Bernard, and Joseph Sherma. *Thin-Layer Chromatography (Chromatographic Science, V. 81)* New York: Marcel Dekker,1999.

ELECTRONIC:

Lawrence Livermore National Laboratory. "Solid-Phase Microextraction." Forensic Science Center. May 6, 2002. <http://www-ems.llnl.gov/s-t/solid_phase.html>(March 5, 2003).

SEE ALSO

Chemical and Biological Detection Technologies
Lawrence Livermore National Laboratory (LLNL)
Toxicology

TIA (Terrorism Information Awareness)

The Terrorism Information Awarness (TIA) system (formerly the Total Information Awareness program) is a new intelligence database system that culls and stores information, and creates risk assessments for a variety of security and intelligence uses. Using communications and financial surveillance, as well as general intelligence information, the TIA system is able sort information, identify patterns, and create data models. System developers predicted its use in security operations ranging from predicting terrorist attacks, to pre-flight screening of airline employees and passengers. The new program, developed by the Defense Advanced Research Projects Agency and managed by the Department of Homeland Security as part of the sweeping post-September 11 security reform, is controversial.

Critics fear that TIA facilitates the government's ability to create dossiers on average citizens. The Department of Defense pressed for the inclusion of medical, financial, and email records in the database. The collection of such personal information without cause or due process, raised questions about the system's implications on 4th Amendment search and seizure provisions.

TIA advocates, including U.S. Attorney General John Ashcroft, claim the system will promote a more thorough and rapid assessment of data, aiding international antiterrorism measures. Opponents of the program assert that the database stores personal information, such as credit reports and organizational affiliations, violating privacy. Many also doubt that use of the TIA system will be limited to terrorist detection, infrastructure protection or other similar measures.

The debate over TIA (then known as the Total Information Awareness program) reached the Senate floor in January 2003, where legislators voted 100–0 to block immediate implementation of the system. The Senate barred the use of the system unless mandated by Congress after a thorough review of its implications for constitutional rights and legal entitlements to privacy.

Upon further deliberation in February, Congress and the Senate negotiated a deal in which TIA could possibly be used outside the United States by military and civilian intelligence forces, specifically for the identification of terrorist threats and the prevention of terrorism. The Wyden Amendment, named after the sponsoring Oregon senator, prohibited the domestic use of TIA technology and created a formal oversight process to review the impact of TIA operations. The Department of Defense was directed provide a full assessment of the possible implication of TIA technology, or halt the program completely.

Although research continues on TIA functions, the future of the TIA program is pending as of May 2003. The Department of Defense, FBI, CIA, and Office of Homeland Security continue to advocate further development, and ultimately implementation, of TIA systems.

SEE ALSO

APIS (Advance Passenger Information System)
DOD (United States Department of Defense)
Homeland Security, United States Department

Tissue-Based Biosensors

The military recognizes that biological cells are excellent sensors of changes in the environment because they respond to external stimuli with highly reproducible and specific signals. Some toxins cause cells to release oxygen radicals or nitrogen products. Other toxins result in the production of biochemical markers, such as enzymes or growth factors. Toxins may also induce structural or morphologic changes in cells. When cells are embedded in three-dimensional tissue constructs, they not only signal the presence of biological or chemical agents, but can also further indicate physiological consequences of exposure to these analytes.

The Defense Advance Research Projects Agency (DARPA) has initiated the Tissue-Based Biosensors Project, which provides funding to research and private institutions to develop two- and three-dimensional tissue-based biosensors that will accurately and efficiently determine of the presence of biological and chemical weapons. The project specifically seeks to develop cell-based systems that can identify human health risks in the battlefield, improve the performance of cells for detection of chemical and biological weapons, enhance and extend the life of cells used as biosensors and impede the degradation of cellular biosensors when in operational use.

A variety of cell types can be used as biosensors, however, because of their inherent electrochemical nature, a majority of the research in the project focuses on developing neural cells and tissues as biosensors. One group, however, is studying physiological changes in bacteria known as extremophiles, because of their ability to withstand harsh environmental conditions. The systems that result from the research may take the form of three-dimensional scaffolds that harbor and nourish detector cells or flow through systems that identify signal cells. Some of the issues that researchers will address while working on this project include nutrient requirements for cells, transport mechanisms for nutrients and wastes, spatial requirements for cells within a three-dimensional matrix, cell signal detection and stability of tissue-based systems. New materials for culturing and maintaining cells in three-dimensional scaffolds will likely be developed.

FURTHER READING:

ELECTRONIC:

Defense Advanced Research Projects Agency. "Tissue-Based Biosensors" <http://www.darpa.mil/dso/thrust/biosci/Tbb/index.html> (March 3, 2003).

SEE ALSO

Biodetectors
Bio-Engineered Tissue Constructs
Biological and Biomimetic Systems
Biological Input/Output Systems (BIOS)
Biosensor Technologies
DARPA (Defense Advanced Research Projects Agency)

Tokyo Rose

ADRIENNE WILMOTH LERNER

During the Second World War, both Allied and Axis nations engaged in a multi-media propaganda battle. Leaflets, posters, film reels, and radio broadcasts were all used to spread misinformation and undermine the morale of enemy troops. Japanese Radio Tokyo broadcast an English language, anti-Allied program entitled the "Zero Hour." The program featured popular music and propagandist war reports read by women with alluring voices. While Radio Tokyo employed over 20 women on the program, the voices became collectively known among Allied soldiers as Tokyo Rose.

Though the moniker Tokyo Rose was popular legend, after the war, details of the Japanese Radio Tokyo propaganda program emerged that brought legend to life. An investigation revealed that Allied prisoners of war, under orders of their captors, produced "Zero Hour." The women who voiced the programs were mostly Japanese citizens. One of the women, however, was an American citizen. This changed the nature of the military investigations from a general inquiry to a treason case.

Iva Ikoku Toguri was born in California in 1916, a first-generation American citizen of Japanese descent. She attended the University of California, Los Angeles, and graduated in 1941. Shortly after graduation, Toguri went to Japan at her mother's request to care for a sick relative. Leaving in haste, she neglected to obtain an official passport that would aid her return to the United States. While in Japan, the Japanese military launched an attack on the American Pacific fleet at Pearl Harbor, bringing America into the Second World War. After war was declared on Japan, Toguri was denied her request to return to the United States. She refused to renounce her American citizenship, and was often placed under surveillance by the Japanese government as a possible enemy operative. Toguri spoke very little Japanese and from 1941 to 1943, she went to school to learn the language. She later took a job as a typist for Radio Tokyo in 1943. Because she knew English, Japanese executives at Radio Tokyo recruited her to voice the "Zero Hour" program. Toguri broadcast under the name Orphan Ann, and worked on the show until the end of the war.

Several war correspondents sought to find and interview the illusive, legendary, Tokyo Rose after the war. A

Iva Toguri D'Aquino, also known as Tokyo Rose, on her way to court in San Francisco, California in 1949, where she was on trial for treason and broadcasting propaganda to Allied troops during World War II. AP/WIDE WORLD PHOTOS.

colleague led reporters to Toguri, after accepting money offered by reporters for the interview. Assuming she had committed no crime as the broadcasts were directed and produced by prisoners of war, Toguri spoke freely with journalists about her role on Radio Tokyo. Conflicting reports exist about her reception of the nickname Tokyo Rose. The press about Toguri, along with the detailed notes of a couple of reporters, was brought to the attention of U.S. Army counter-intelligence.

United States Army authorities arrested Toguri in 1945. In 1948, she was brought to the United States and transferred to officers of the Federal Bureau of Investigation. After a five-year inquiry, Toguri was tried as the infamous Tokyo Rose on eight counts of treason. Acquitted of seven counts of treason, she was found guilty on the remaining charge of "speaking about the location and destruction of ships." She was sentenced to ten years in prison and a steep monetary fine. When released in 1956, she immediately sought to clear her name. She applied twice for a presidential pardon, but was denied.

The matter of Tokyo Rose disappeared from the public eye until a journalist in the 1970s probed for further information on the case. A series of articles revealed several incongruencies in the inquiry and trial of Toguri. Prosecutors argued that Toguri fled the United States before the war and was possibly a Japanese intelligence agent, but scant evidence was offered. Testimonies of several Allied service members regarding the radio broadcasts were revisited, and Japanese records regarding the Radio Tokyo psychological warfare campaign were unearthed. Interviews of some of Toguri's wartime colleagues corroborated her earlier claims that she sometimes smuggled supplies and food for the Allied prisoners also employed on the "Zero Hour" program. Further interviews and documents revealed that information regarding ships and troop positions that Radio Tokyo broadcast was available in wartime America on short-wave radio and was selected by the POWs forced to work on the program because it was not immediately sensitive to the Allied war effort. The controversial treason case was never reopened by courts, but Toguri was issued a pardon by President Gerald Ford, in one of his last presidential acts, in 1977.

FURTHER READING:

BOOKS:

Duus, Masayo, and Edwin O. Reischauer. Peter Duus (trans.) *Tokyo Rose: Orphan of the Pacific* Tokyo: Kodansha International, 1979.

SEE ALSO

Propaganda, Uses and Psychology
World War II

Tournament of Shadows.

SEE *Great Game.*

Toxicology

JUDYTH SASSOON

The science of toxicology is concerned with the adverse effects of chemicals on biological systems and includes the study of the detection, action and counteractions of poisons. Toxicologists today generally use the techniques of analytical chemistry to detect and identify foreign chemicals in the body, with a particular emphasis on toxic or hazardous substances. Toxins can be simple metal ions or more complex, inorganic and organic chemicals, as well as compounds derived from bacteria or fungi and animal-produced substances such as venoms. Poisons can range in their effects from a low-level debilitation to almost immediate death. Many drugs used to counter diseases can also be poisons at higher concentrations.

One of the most significant historical figures in the development of the science of toxicology was the Swiss physician and alchemist Paracelsus (1493–1541). He realized that there was a need for proper experimentation in the field of chemical therapeutics and distinguished between the therapeutic and toxic properties of substances, recognizing that they are indistinguishable except by dose. Paracelsus realized that it is not possible to categorize chemicals as either safe or toxic and laid the foundations for a key principle in toxicology known as the dose-response relationship. There is a graded dose-response relationship in individuals and a quantal dose-response relationship in a population. The quantal "all or none" dose-response is used to determine the median lethal dose (LDm), which estimates what percentage of the population, would be affected by a dose increase. Estimation of LDm involves the use of at least two different animal species and doses of the chemical under test are administered by at least two different routes. Initially most of the test animals die within 14 days. Subacute exposure is then tested for a period of 90 days and long-term exposure testing takes a further 6 months to 2 years. Mathematical extrapolation is used to generalize results from animal testing to human risk incidence.

Another significant figure in toxicology was Spanish physician Orfila (1787–1853) who contributed to the specialty known as forensic toxicology. He devised methods of detecting poisonous substances and therefore provided the means of proving when criminal poisoning had taken place. After Orfila, toxicology developed further to include the study of mechanisms of poison action.

Forensic toxicology involves the use of toxicological methods for legal purposes. There is a considerable overlap between forensic and clinical toxicology, criminology, forensic psychology, drug testing, environmental toxicology, pathology, pharmacology, sports medicine and veterinary toxicology. The work of a forensic toxicologist generally falls into three main categories: identification of drugs such as heroin, cocaine, cannabis; detection of drugs and poisons in body fluids, tissues and organs; and measuring of alcohol in blood or urine samples. Results of the laboratory procedures must then be interpreted and presented to the legal courts.

A forensic toxicologist is normally given preserved samples of body fluids, stomach contents, and organ parts along with a coroner's report containing information on symptoms and postmortem data. Specimens are generally divided into acidic and basic fractions for drug extraction from tissue or fluid. As an example, most of the barbiturate drugs are acid-soluble while most of the amphetamine drugs are base-soluble. After preliminary acid-base procedures, tissue or fluid samples are subjected to further laboratory tests consisting of screening tests and confirmation testing. Screening tests allow the processing of many specimens for a wide range of toxins in a short time and any positive indications from the screens are then verified with a confirmation test.

Laboratory methods used in toxicological analysis are various. Screening tests include (1) physical tests: testing the boiling point, melting point, density, and refractive index of a substance; (2) crystal tests: treatment of a substance with a chemical reagent to produce crystals; (3) chemical spot tests: treatment with a chemical reagent producing color changes; (4) chromatographic tests (thin layer or gas): these separate the mixtures under investigation. Confirmatory tests generally involve mass spectrometry in combination with gas chromatography. Every toxin has a characteristic mass spectrum that identifies it absolutely.

Drugs analysis in tissue samples can be very complicated and a substance under analysis must be subjected to rigorous tests with no margin for error. A range of screening tests employing color reactions exist for the detection of illegal drugs. Some commonly used color tests include the Marquis test for opium, Duqunois-Levine test for Marijuana, Van Urk test for LSD, Scott test for cocaine, and Dillie-Koppanyi test for barbiturates.

The challenges of modern science call on clinical and forensic toxicologists to expand their services. They are now encouraged to engage in research and development to meet a number of changing needs. Modern molecular biology has opened up a number of interesting possibilities for toxicologists. For example, genotyping for interpretation of potential toxic drug interactions and criminality testing is becoming a field of great interest. With the emergence of pharmacogenetics, genotyping may enhance rational drug therapy for better patient care, and may explain unexpected adverse or fatal drug reactions in postmortem analysis.

Expanding responsibilities for forensic toxicologists also derive from the greater threat of terrorism. Terrorism via weapons of mass destruction has moved out from war zones to civilian settings. Modern terrorist weapons may be in the form of nuclear, biological, and chemical devices. Recently, the possible use of chemical or biological weapons in the Middle East conflicts, the use of sarin gas in a Tokyo subway station, and the unregulated availability of nuclear fuel in some countries have all heightened the potential risks. Toxicologists must now be knowledgeable about the clinical pharmacology, safe samples processing, and possible screening and/or analysis of substances such as vesicants, cyanide, nerve agents, and riot control agents.

FURTHER READING:

BOOKS:

Bodziak, J., and Jon J. Nordby. *Forensic Science: An Introduction to Scientific and Investigative Techniques.* CRC Press, 2002.

Klaassen, C. D. *Toxicology: The Basic Science of Poisons.* McGraw-Hill Companies, 2001.

PERIODICALS:

Goldberger, B. A., and A. Polettini. "Forensic Toxicology: Web Resources." *Toxicology* 173 (2002): 97–102.

Maurer H. H. "Liquid Chromatography-mass Spectrometry in Forensic and Clinical Toxicology." *J Chromatogr B Biomed Sci Appl.* 713 (1998): 3–25.

Richardson T. "Pitfalls in Forensic Toxicology." *Ann Clin Biochem.* 37 (2000): 20–44.

Thormann, W., Y Aebi, M. Lanz, and J. Caslavska "Capillary Electrophoresis in Clinical Toxicology." *Forensic Sci Int.* 92 (1998): 157–83.

Wong, S. H. "Challenges of toxicology for the millennium." *Ther Drug Monit.* 22 (2000): 52–7102.

SEE ALSO

Chemical and Biological Detection Technologies
Chemistry: Applications in Espionage, Intelligence, and Security Issues
Drug Control Policy, United States Office of National Forensic Science
Thin Layer Chromatography

Toxins

BRIAN HOYLE

Toxins are compounds that are produced and released by a variety of microorganisms and other organisms. Toxins can be fast-acting and, because they are already preformed, do not require the growth of a microorganism in the host. State-sanctioned weaponization programs for various toxins have occurred in the past in many countries, and may be ongoing. As well, toxins are a potent weapon for terrorists.

Bacterial toxins. Toxins are the main disease-causing factor for a number of bacteria. Some examples include *Corynebacterium diphtheriae* (diptheria), *Vibrio cholerae* (cholera), *Bacillus anthracis* (anthrax), *Clostridium botulinum* (botulism), certain strains of *Escherichia coli* (hemolytic uremic syndrome), and *Staphylococcus aureus* (toxic shock syndrome).

Certain species of these bacteria are of particular concern in biological warfare and biological terrorism. As the events of 2001 in the United States demonstrated, powdered preparations of *Bacillus anthracis* spores was easily delivered to a target through the mail. The dispersal of the spores in the air and the inhalation of the spores can cause a form of anthrax that develops quickly and, without treatment, is almost always fatal. The bacteria in the genus *Clostridium* also form spores. Additionally, during the 1990s, a strain of *Staphylococcus aureus* emerged that is resistant to almost all known antibiotics.

Bacterial toxins have a wide variety of activity. Some toxins damage the cell wall of host cells, either by dissolving the wall or by chemically punching holes through the wall. Examples of such toxins are the alpha toxin of *Clostridium perfringens*, hemolysin of *Escherichia coli*, and streptokinase of *Streptococcus pyogenes*. The damage to the host cells allows the bacteria to spread rapidly through the host. This can cause an overwhelming infection.

Other bacterial toxins kill host cells by stopping the manufacture of protein in host cells or by degrading the proteins. Examples of protein blockers include exotoxin A of *Pseudomonas aeruginosa* and the Shiga toxins produced by both *Escherichia coli* and *Shigella dysenteriae*. Protein degrading toxins include those produced by *Bacillus anthracis* and *Clostridium botulinum*

Still other toxins stimulate an immune response of the host that is so strong that it can damage the host. *Staphylococcus aureus* produces at least three different toxins that have this effect (i.e., toxic shock syndrome).

Marine toxins. Microorganisms called dinoflagellates can produce toxins when they grow in species of shellfish. Usually, the toxins are a concern when the contaminated seafood is inadvertently eaten. But, the toxins can be isolated in pure form. The purified toxins will produce illness when deliberately used.

Aflatoxin. Aflatoxin is produced by two species of mold—*Aspergillus flavus* and *Aspergillus parasiticus*. The toxin is especially a concern when potatoes are contaminated by the mold. Ingestion of the contaminated potatoes can cause serious, even fatal illness. This toxin is of particular concern for food supplies. Storehouses of produce like potatoes are susceptible to the malicious release of the molds.

Ricin. Ricin is a toxin that is produced by the castor bean. It is the third most deadly toxin that is known, after the toxins produced by *Clostridium botulinum* and *Clostridium tetani*. The symptoms of ricin toxin include nausea, muscle spasms, severe lung damage, and convulsions. These symptoms appear within hours, and, without treatment, death from pulmonary failure can result within three days. There is no vaccine or antidote for the toxin.

Ricin has long been a weapon of espionage and terrorism. The most famous use of ricin occurred in 1978, when Georgi Markov—a recently defected Bulgarian official—was killed by KGB agents on a bridge in London. An umbrella tip was used to inject a capsule of ricin into one of his legs.

The planned use of ricin by al-Qaeda has been alleged. Traces of ricin have been found in caves in Afghanistan that were used by al-Qaeda. Iraq is also suspected of using ricin in its weaponization program of the 1990s.

Also, in January 2003, British antiterrorism officers seized a quantity of ricin in London from a group of Algerian men suspected of being terrorists.

Toxoid vaccines. Some toxins that are capable of causing much harm are also a source of protection. Because of its potency, a toxin cannot be used protectively in its unaltered form. Toxins can be altered, however, so that they do not produce the undesirable effects, but which still stimulate the immune system to produce antibodies to a critical part of the toxin molecule. The weakened version of a toxin is called a toxoid.

The anthrax vaccine that is currently licensed for use contains two toxoids in addition to other immune stimulating molecules. The immune response will produce antibodies to the two toxins of the anthrax bacterium.

FURTHER READING:

PERIODICALS:

Schmitt, C. K., K. C. Meysick, and A. D. O'Brien. "Bacterial Toxins: Friends or Foes?" *Emerging Infectious Diseases* no. 5 (1999): 224–34.

ELECTRONIC:

Centers for Disease Control and Prevention. "Marine Toxins." Division of Bacterial and Mycotic Diseases. June 10, 2002. <http://www.cdc.gov/ncidod/dbmd/diseaseinfo/marinetoxins_g.htm>(29 January 2003).

United States Department of Agriculture. "Aflatoxin." USDA Grain Inspection, Packers and Stockyards Administration. September 17, 1998. <http://www.usda.gov/gipsa/newsroom/backgrounders/b-aflatox.htm>(29 January 2003).

University of Wisconsin at Madison. "Mechanisms of Bacterial Pathogenicity: Protein Toxins." Bacteriology at UW-Madison. 2002. <http://www.bact.wisc.edu/Bact330/lecturept>(30 January 2003).

SEE ALSO

Biocontainment Laboratories
Biosensor Technologies
Food Supply, Counter-terrorism

Tradecraft

Operatives of intelligence services and other covert organizations use the term *tradecraft* to refer to the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business. Elements of tradecraft, in general terms, include the ways in which an intelligence officer arranges to make contact with an agent, the means by which the agent passes on information to the officer, the method for paying the agent, and the many precautions and tactics of deception applied along the way.

Examples of tradecraft can be found in the Ashenden stories, through which British author Somerset Maugham recounted, in fictional form, his experiences as a spy in World War I. In one tale, for instance, Maugham mentioned that Ashenden met an "old butter-woman" regularly in a market in Geneva. The woman was actually an agent of British intelligence who, in real life, passed notes back and forth between Maugham and his superiors in London. This is tradecraft in its simplest form—the employment of someone or something that is not exactly who or what he/she/it seems to be.

Another example of tradecraft in action is the artwork of Robert Baden-Powell who, long before he founded the Boy Scouts, served as a military intelligence officer in the Balkans during the 1890s. In order to sketch enemy fortifications without attracting attention, Baden-Powell adopted the disguise of an entomologist. He made detailed sketches of butterflies and leaves that, on close scrutiny, were revealed to be maps of gun emplacements or trenches.

Tradecraft can also include the many precautions taken to avoid detection in the process of making a drop, or otherwise transferring material between agent and officer, as in Maugham's case of the old butter-woman. In real life, Soviet agent John made his drops using a garbage bag that included bits of recognizable trash—but nothing that would smell strongly, attract animals, or cause damage to the documents and other important materials he left for his KGB handlers.

FURTHER READING:

BOOKS:

Carl, Leo D. *The CIA Insider's Dictionary of U.S. and Foreign Intelligence, Counterintelligence, and Tradecraft.* Washington, D.C.: NIBC Press, 1996.

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Nash, Jay Robert. *Spies: A Narrative Encyclopedia of Dirty Deeds and Double Dealing from Biblical Times to Today.* New York: M. Evans, 1997.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

SEE ALSO

Cambridge University Spy Ring
Cameras
Cameras, Miniature
Concealment Devices
Dead Drop Spike
Dead-Letter Box
Hanssen (Robert) Espionage Case
Intelligence Agent
Intelligence Officer
Walker Family Spy Ring

United States soldiers, left, stand watch in Grand Central Terminal in New York after the Transportation Department warned transit and other railroad systems about possible terrorist attacks in May 2002. AP/WIDE WORLD PHOTOS.

Transportation Department, United States

A vital part of America's critical infrastructure, the United States Department of Transportation (DOT) was established by an act of Congress in 1966 and began operation on April 1, 1967. Today the DOT comprises a number of bureaus and offices designed to promote efficiency and safety in air, road, rail, and marine travel and transport throughout the nation. The mission of DOT is to develop and coordinate policies to provide efficient, economical national transport systems whose operations take into account economic, environmental, and national security needs.

Agencies of DOT. In addition to the Office of the Secretary, DOT consists of 11 individual operating agencies. Among these are the Federal Aviation Administration, which oversees the safety of civil air transport. DOT was also home to the Transportation Security Administration, created in the wake of the 2001 terrorist attacks to provide aviation security, and the U.S. Coast Guard. Both were transferred to the newly created Department of Homeland Security in March 2003. Sea borne components of DOT include the Maritime Administration, which promotes the development and maintenance of the U.S. merchant marine, and the Saint Lawrence Seaway Development Corporation, which maintains the waterway between the Great Lakes and Atlantic Ocean.

Areas of DOT devoted to highways and railroads include the Federal Highway Administration, which coordinates inter- and intrastate highway programs and manages roads on federal lands such as national forests and Indian reservations; the Federal Motor Carrier Safety Administration, established in 2000 to reduce commercial motor vehicle-related fatalities and injuries; the Federal Railroad Administration, which promotes safe and environmentally sound rail transport; the Federal Transit Administration, which assists cities and communities in developing and improving mass transit systems; and the National Highway Traffic Safety Administration, which is responsible for reducing deaths and economic losses from motor vehicle crashes.

Other agencies of DOT are the Research and Special Programs Administration, which oversees the transport of

hazardous materials; the Bureau of Transportation Statistics, which collects data on transport and travel, and works closely with the Bureau of the Census in the Commerce Department; and the Surface Transportation Board, which is responsible for economic regulation of interstate surface transportation, primarily railroads. The last of these is an independent body organizationally housed within DOT.

FURTHER READING:

BOOKS:

National Transportation Strategic Research Plan. Washington, D.C.: National Science and Technology Council, 2000.

U.S. Department of Transportation Research and Development Plan. Washington, D.C.: John A. Volpe National Transportation Systems Center, 1999.

Whitnah, Donald Robert. *U.S. Department of Transportation: A Reference History.* Westport, CT: Greenwood Press, 1998.

ELECTRONIC:

U.S. Department of Transportation. <http://www.dot.gov/> (April 3, 2003).

SEE ALSO

Air Marshals, United States
Aviation Security Screeners, United States
Civil Aviation Security, United States
Coast Guard (USCG), United States
Critical Infrastructure
FAA (United States Federal Aviation Administration)
Homeland Security, United States Department
NTSB (National Transportation Safety Board)
Port Security

Treasury Department, United States

MARTIN J. MANNING

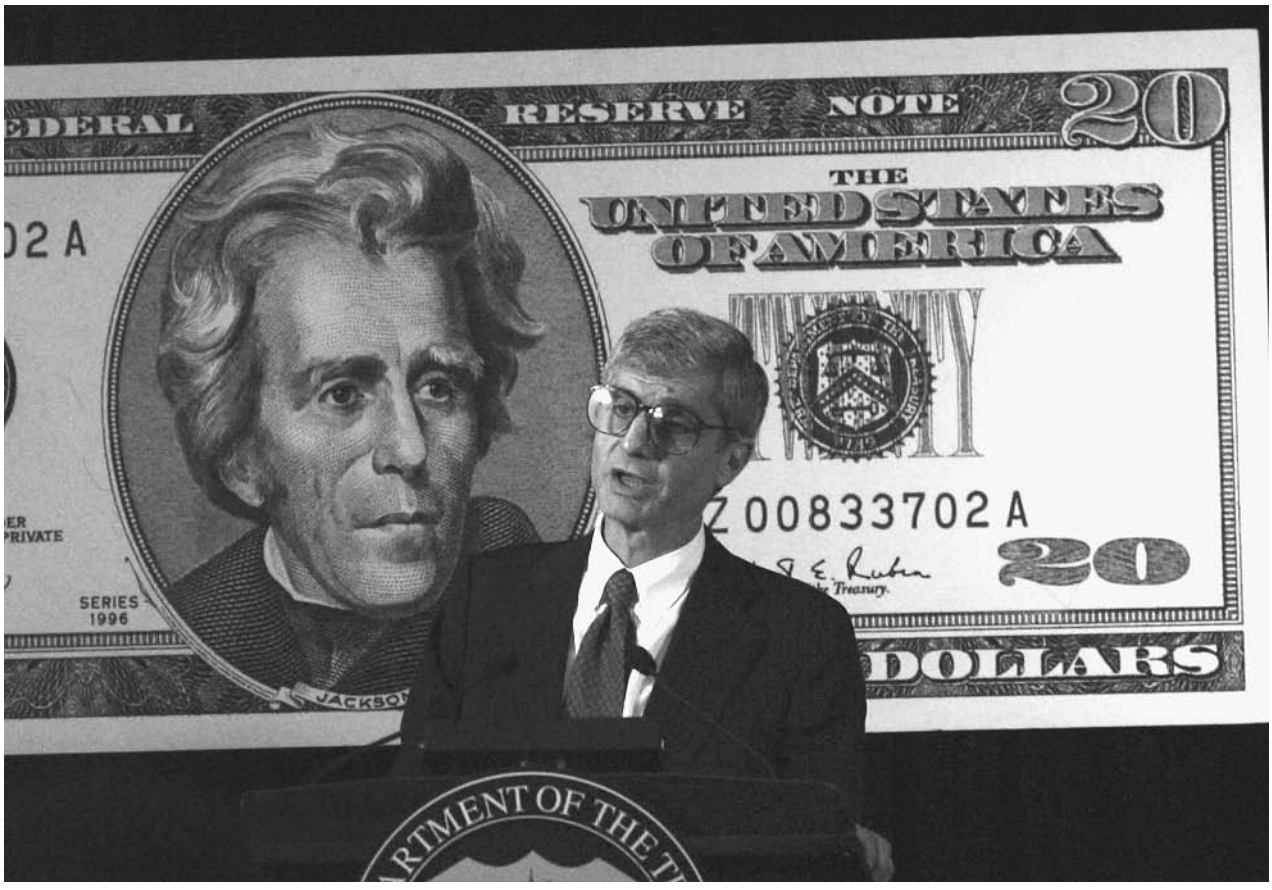
The United States Department of the Treasury, the second-oldest department in the U.S. Government, was established by an Act of Congress on 2 September 1789 (I Stat. 65; 31 U.S.C. 1001). It advises Congress and the president on tax policy, acts as financial agent for the federal government, manufactures currency, and enforces tax laws. According to its establishment legislation, the Treasury Department is to "formulate, recommend, and administer domestic and international financial, economic, and tax policies, and manage the public debt." The Department serves as the principal financial agent for the United States government, manufactures coins and currency, and oversees the administration of the U.S. Customs Service (1789), U.S. Mint (1792), Internal Revenue Service (1862), Bureau of Engraving and Printing (1862), Office of the Comptroller of the Currency (1863), Secret Service (1865), Bureau of the Public Debt (1919), Financial Management Service (1920), Federal Law Enforcement Training Center (1970), Bureau of Alcohol, Tobacco, and Firearms (1972), and Office of Thrift Supervision (1989).

Background. The Treasury Department was already in existence in some form during the War of American Independence. On June 22, 1775, the Second Continental Congress approved the printing of $2 million in bills of credit to finance the War of American Independence. Between 1775 and 1779, more than $241 million Continentals were issued. The value of this first national paper money fell so low it engendered the expression "not worth a Continental." A month later, July 29, 1775, the Continental Congress appointed joint treasurers (Michael Hillegas and George Clymer). That November, a committee was established by the Continental Congress to examine the money in the Treasury and to estimate the public debt. The committee was one of several established by the Congress to handle different phases of the revolutionary finances. In February 1776, a standing committee of five was appointed to superintend the Treasury. The committee was referred to by various names, including Board of Treasury and Treasury Office of Accounts.

On July 31, 1789, the collection of customs revenue was established when the Tariff Act became effective. A Bureau of Customs, later the U.S. Customs Service, was created by an act of March 3, 1927 (44 Stat. 1381); 19 U.S.C. 2071). A postal service was established by Congress on September 22, 1789.

With the establishment of the Treasury Department, the first Secretary of the Treasury, Alexander Hamilton, maneuvered to give the emerging United States a strong financial basis and to provide the stability needed for economic development. Hamilton worked to fund the national debt, assume the state debts, create a national bank, pass a whiskey tax, enact high tariffs, and establish American industry on a sound financial footing. He was aided by legislation (April 2, 1792) that established a national mint and regulated coinage and an act (May 8, 1792; revised Act of March 3, 1809, chap. 28) that organized the Department of the Treasury into two major components: the Departmental offices, primarily responsible for the formulation of policy and management of the Department as a whole, and the operating bureaus, which carry out the specific operations assigned to the Department. Today, the bureaus make up 98% of the Treasury work force.

Key developments. Congress approved legislation (June 23, 1836) that required the Secretary of the Treasury to designate at least one bank in each state and territory for the



Treasury Secretary Robert Rubin holds a 1998 press confernce to announce the release of a new $20 bill, redesigned to include features that make it more difficult to counterfeit. Anti-counterfeit features will be enhanced every seven to ten years, and will include subtle color changes. AP/WIDE WORLD PHOTOS.

deposit of government funds. Six years later, on Independence Day, sub-treasuries for deposit of federal funds were authorized in major cities but the legislation was repealed the next year (1841).

The Civil War (1861–1865) was the first modern war demanding enormous capital. The cost, after four years, was $2.3 billion to the U.S. government and $1 billion to the Confederacy. Less than one-fifth of the North's cost was paid for in taxes; four-fifths was financed by borrowing and the issue of unredeemable paper currency. To remedy this, and to set up future reserves, the Revenue Act (12 Stat. 432; 26 U.S.C. 3900; July 1, 1862) established a permanent tax collection agency, Commissioner of Internal Revenue, although internal taxes were levied by Congress and collected by the Treasury Department from 1791 to 1802 and 1813 to 1817. To administer the national banks, the Office of the Comptroller of the currency was created by legislation (12 Stat. 665; February 25, 1863). However, a national tragedy led to the creation of one of the better-known Treasury bureaus when the U.S. Secret Service, oldest general law enforcement agency in the federal government, was established (July 5, 1865) after the Lincoln assassination. Along with its protection of presidential families, heroically documented in stage screen, and print, the Secret Service was also authorized to halt the counterfeiting of currency. It derives its authority from the act of June 23, 1860 (12 Stat. 102). Today, it still provides these services although its detection of counterfeit money and its arrest of counterfeiters continues to fall behind its rather more popular and visual image of Secret Service agents traveling with the president and other VIPs.

"Guns and Butter" diplomacy. World War I cost $32.7 billion. To finance this enormous cost, President Wilson and Treasury Secretary William G. McAdoo transformed the income tax into the foremost instrument of federal taxation, both to raise revenue and to attack concentrations of wealth, special privilege, and public corruption; and to promote a more competitive economy. The Revenue Acts (1916, 1917) [39 Stat. 756, 1000] imposed the first significant taxes on corporate profits and personal incomes and introduced a graduated federal estate tax, but rejected a mass-based income tax. An excess profits tax became the centerpiece of wartime finance.

Henry Morgenthau, President Franklin Roosevelt's Secretary of the Treasury, issued regulations in 1934 that established a reporting system for specified international

capital movements. Along with the required reports on security and foreign exchange transactions and changes in bank balances between the United States and foreign countries, commercial and industrial firms reported their foreign assets and liabilities. The present Treasury International Capital reporting system, an ongoing statistical program, evolved from the 1934 data collection efforts.

World War II, the most costly in American history at $360 billion, changed the American tax system as it shifted from a narrow base to a broad base, the basis of our current tax system. Roosevelt and Morgenthau wanted to finance the war with taxes that came mostly from business and upper-income groups as nearly one-half of America's national product went to war. Along with lend-lease programs, Treasury designed and implemented Foreign Funds Control (1940) to protect in the U.S. the assets of invaded countries and to keep them from the enemy. Foreign Funds Control froze Axis assets in 1941, regulated international financial transactions, administered wartime trade restrictions (Trading with the Enemy Act), and froze $8.5 billion of assets belonging to thirty-five countries by war's end. Although liquidated in 1948, Foreign Funds Control was re-established in 1950 as Foreign Assets Control.

Production of military invasion currency was among the Treasury's most highly secret work since any knowledge of production would reveal Allied invasion plans. Treasury loaned 14,000 tons of silver to help produce uranium for the atom bomb and financed the top-secret Manhattan Project while Morgenthau and a group of Treasury attorneys persuaded Roosevelt to establish the War Refugee Board (1944), the only government effort to save European Jews.

In the post-World War II period, Treasury developed international monetary policy to aid countries devastated by the war but by the end of the Korean War, the U.S. American dominance was lessening as it began to compete for economic control with countries it originally assisted. Treasury, supported by other U.S. agencies, developed comprehensive proposals for the reform of the international monetary system after fiscal collapses in the 1960s and the 1970s. Strengthened by accords and agreements, Treasury developed further policies to resolve the international debt crises of the 1980s and the early 1990s. Since 1989, Treasury has guided U.S. participation in the Financial Services negotiations of the Uruguay Round multilateral talks under the General Agreement on Trade in Services and the World Trade Organization.

After the terrorist attacks of September 11, 2001, the Treasury Department implemented regulations for helping financial institutions comply with the USA PATRIOT Act, a comprehensive legislative enactment addressing many facets of terrorist financing and money laundering passed by Congress after the terrorist attacks. The Department works jointly with other federal agencies to craft effective and common-sense regulations and programs that will help industry guard against future terrorist infiltration and abuse.

To date, the Treasury Department has issued a number of proposed and interim rules to help the financial services industry address specific threats to the financial system, create anti-money laundering programs that are tailored to each industry's needs, alert the appropriate authorities to large or suspicious financial transactions, and better understand their relationship with foreign banks. At the beginning of the twenty-first century, Treasury continues to maintain a central position within the federal government due to its size, leadership, and important role in the economic development of the United States.

FURTHER READING:

BOOKS:

Gilbert, Abby L. "Treasury, Department of the." In: Kurian, George T., ed. *A Historical Guide to the U.S. Government.* New York and Oxford: Oxford University, 1998.

Katz, Bernard S., and C. Daniel Vencill, eds. *Biographical Dictionary of the United States Secretaries of the Treasury, 1789–1995.* Westport, CT: Greenwood, 1996.

Walston, Mark. *The Department of the Treasury.* New York: Chelsea House, 1989.

ELECTRONIC:

U.S. Department of the Treasury Department<http://www.ustreas.gov> (April 18, 2003).

SEE ALSO

Internal Revenue Service, United States
Secret Service, United States

Truman Administration (1945–1953), United States National Security Policy

CARYN E. NEUMANN

The onset of the Cold War during the presidency of Harry S. Truman led the executive branch recognize a need to integrate domestic, foreign, and military policies to combat the expansionism of the Soviet Union. The Truman Doctrine set the major goal of the U.S. as opposition to communism anywhere in the world. The Marshall Plan, the Organization of American States (OAS), and the National Security Council (NSC) all served as part of the administration's unified approach to the immense challenges posed by the expansion of communism.

Harry S. Truman took office upon the sudden death of Franklin D. Roosevelt in April 1945. The new president

continued with much of the Roosevelt administration's diplomacy, but had always been far sterner than Roosevelt toward the Soviet Union. He also had to plan for a postwar world and the primary concern of the postwar Truman administration was to prevent a repeat of the Great Depression. American officials held that another economic downturn could only be avoided if global markets and raw materials were fully open to all peoples on the basis of equal opportunity. On the other hand, Josef Stalin, dictator of the Soviet Union, demanded that the U.S. recognize the Soviet right to control large parts of Eastern Europe. These Soviet satellite states would serve as a strategic buffer against the West that could also be exploited economically for the rapid rebuilding of the devastated Soviet economy. Truman refused to comply with the wishes of the Soviets and the Cold War gradually took root.

By 1946, the administration had become deeply concerned about the consolidation and development of Russian power. One year later, in 1947, Truman issued a declaration that would serve as the guiding force of national security policy for the duration of the Cold War. With the Truman Doctrine, he asked Americans to join in a global fight against communism. He committed the U.S. to opposing totalitarian regimes and supporting freedom, while refusing to place any geographical limits upon this obligation. Several days after the speech, the president announced a loyalty program to ferret out security risks in government. The first such peacetime program in U.S. history, it was so vaguely defined that political ideas and long-ago associations were suddenly made suspect.

The overwhelming fear of communism at home and abroad would convince Americans to support a national security policy that included intervention in the affairs of other countries. The end of World War II confronted the United States with the problem of reconstructing Europe. Most of Europe lay in shatters, with countries too weak to readily rebuild the infrastructure necessary for economic growth. In order to prevent a collapse of the European economy and the ramifications on the economy of America, the Truman administration began a massive economic aid effort. The 1948 Marshall Plan, named for Secretary of State George C. Marshall, offered aid to all of Europe with the provision that the Europeans determine their own needs. Before its end in 1951, the plan prevented poverty and chaos from overwhelming Western Europe. The Soviets, suspicious of American aims, declined to participate.

In order to prevent communist aggression around the world, the U.S. joined with its neighbors to the south in a mutual security agreement. The nations of the Western Hemisphere convened in Rio de Janeiro, Brazil in 1947 to sign the Rio Treaty for collective self-defense. The agreement provided that an attack upon one nation in the Americas served as an attack upon them all. If two-thirds of the countries agreed to resist an attack, all states must cooperate by sending either troops or supplies. In 1948, the U.S. participated in the formation of the Organization of American States (OAS). The administration hoped that the OAS would eventually assume the mounting responsibilities for solving hemispheric problems, but the U.S. would always play the dominant role.

By 1947, the various means of security planning had fully emerged and ranged from economic planning through diplomatic initiative to application of military force. The missing element was a forum in which to select the appropriate combination of measures for a particular situation. Truman generally relied upon Special White House Counsel Clark Clifford to provide day-to-day coordination. Clifford, dismayed by the disorder among agencies involved in major policymaking decisions, played an instrumental role in establishing the National Security Council in 1947 to give institutional stability to national security policymaking.

Until the advent of the Korean War in 1950, Truman remained unenthusiastic about the NSC. Truman saw the NSC as an effort by Congress to harness the president to the advice of military men. He attended only 10 of the first 55 meetings on the grounds that his presence would inhibit frank discussion and suggest that national policies were made by committee. When Truman did participate in NSC gatherings, the council reached conclusions that matched his known desires and ideological inclinations. The complicated situation in war-torn Korea finally convinced Truman of the value of the NSC as a policy development mechanism.

During the Truman administration, the NSC's main products were policy papers. NSC-20/4 served as the basic American strategic plan from 1948 until 1950. This document saw Russian expansionism as part of a massive drive for world mastery. It stated that the U.S. would not attempt an occupation of the Soviet Union but should be prepared for a negotiated peace. American objectives were set as the reduction of the power and influence of the Soviet Union to the point where the U.S.S.R. could no longer mount a threat to world peace.

NSC-68, the replacement for NSC-20/4, is arguably among the most significant of NSC documents. In it, the NSC argued that in the current polarized climate, a defeat of free institutions anywhere in the world damaged the U.S. This belief defined any threat to the capitalist political system as communist-inspired, not as the result of problems within. NSC-68 shocked the government into greater anti-communist resolution and action, thereby setting the stage for involvement in wars in Korea and Vietnam. It also comprised the final attempt of the Truman administration to define national security policy.

In establishing the national security policy and system that would guide the United States for much of second half of the twentieth century, Truman opened the Cold War. Fear of communism and determination to oppose it at every opportunity led to the U.S. involvement in the Korean War as well as McCarthyism.

■ FURTHER READING:

BOOKS:

Boll, Michael M. *National Security Planning: Roosevelt through Reagan.* Lexington: University Press of Kentucky, 1988.

Crabb, Cecil V., and Kevin V. Mulcahy. *American National Security: A Presidential Perspective.* Pacific Grove, CA: Brooks/Cole, 1991.

Graebner, Norman A., ed. *The National Security: Its Theory and Practice, 1945–1960.* New York: Oxford University Press, 1986.

ELECTRONIC:

White House. "History of the National Security Council, 1947–1997" <http://www.whitehouse.gov/nsc/history.html> (April 25, 2003).

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Department of State, United States
Korean War
McCarthyism
National Security Act (1947)
NSC (National Security Council)
National Security Strategy, United States

Truman Doctrine.

SEE *Cold War (1950–1972).*

Truth Serum

■ BELINDA ROWLAND

Truth serum is a term given to any of a number of different sedative or hypnotic drugs that are used to induce a person to tell the truth. Truth serums cause a person to become uninhibited and talkative, but they do not guarantee the veracity of the subject.

In 1943, J. Stephen Horsley published a book in which he described the psychotherapeutic method of narcoanalysis. By chance, he observed that persons who were under the influence of narcotics were uninhibited, talkative, and answered all questions that were asked of them. A narcotic is a drug that dulls the senses, relieves pain, and induces sleep. Persons who were under the influence of narcotics entered a hypnotic-like state and spoke freely about anxieties or painful memories. Once the drug effect had worn off, the person had no recollection of what he or she said. Horseley coined the term "narcoanalysis." Narcoanalysis has since been used to assist in the diagnosis of several different psychiatric conditions.

The term "truth serum" has been applied to drugs that are used in narcoanalysis. This term is a misnomer in two ways: the drugs used are not serums and truthfulness is not guaranteed. Although inhibitions are generally reduced, persons under the influence of truth serums are still able to lie and even tend to fantasize. Courts have ruled that information obtained from narcoanalysis is inadmissible.

Narcoanalysis is not used in the United States as an interrogation method. The Federal Bureau of Investigation (FBI) and other federal law enforcement agencies object to the use of truth drugs, preferring instead to use psychological methods to extract information from suspects or prisoners. The United Nations considers the use of truth drugs to be physical abuse and, therefore, a form of torture. The issue was revisited in 2002, when some authorities, including former Central Intelligence Agency and FBI chief William Webster, frustrated by the lack of forthcoming information from suspected al-Qaeda and Taliban members held at the U.S. prison in Guantanamo Bay, Cuba, advocated administering narcoanalysis drugs to uncooperative captives. United States Secretary of Defense Donald Rumsfeld asserted that narcoanalysis is not used by United States military and intelligence personnel, but suggested that other countries have made use of the technique in the interrogation of suspected terrorists.

Drugs used as truth serums. Two of the most commonly used truth serums are members of the barbiturate drug class. Barbiturates are sedatives and hypnotics that are created from barbituric acid. They are divided into classes according to the duration of sedation: ultrashort, short, intermediate, and long. Ultrashort-acting barbiturates are used as anesthetics whereas long-acting ones are used to treat convulsions (anticonvulsive). Barbiturates are controlled substances due to their high potential for abuse and for addictive behavior.

Sodium pentothal (pentothal sodium, thiopental, thiopentone) is an ultrashort-acting barbiturate, meaning that sedation only lasts for a few minutes. Sodium pentothal slows down the heart rate, lowers blood pressure, and slows down (depresses) the brain and spinal cord (central nervous system) activity. Sedation occurs in less than one minute after injection. It is used as a general anesthetic for procedures of short duration, for induction of anesthesia given before other anesthetic drugs, as a supplement to regional anesthesia (such as a spinal block), as an anticonvulsive, and for narcoanalysis.

Sodium amytal (amobarbital, amylobarbitone, Amytal) is an intermediate-acting barbiturate. Sedation occurs in one hour or longer and lasts for 10 to 12 hours. Sodium amytal depresses the central nervous system. It is used as a sedative, hypnotic, and anticonvulsive and for narcoanalysis. When sodium amytal is used for narcoanalysis it may be called an "Amytal interview."

Scopolamine (hyoscine) is an anticholinergic alkaloid drug that is obtained from certain plants. Anticholinergic

drugs block the impulses that pass through certain nerves. Scopolamine affects the autonomic nervous system and is used as a sedative, to prevent motion sickness, to treat eye lens muscle paralysis (cycloplegic), and to dilate the pupil (mydriatic).

FURTHER READING:

BOOKS:

Horsley, J. Stephen. *Narco-Analysis. A New Technique in Short-Cut Psychotherapy: A Comparison with Other Methods and Notes on the Barbiturates.* New York: Oxford University Press, 1943.

PERIODICALS:

Johnson, K. and R. Willing. "Ex-CIA Chief Revitalizes 'Truth Serum' Debate." *USA Today.* (April 26, 2002): 12a.

Romanko, J.R.."Truth Extraction." *New York Times Magazine.* (November 19, 2000): 54.

SEE ALSO

Polygraphs

Tularemia

BRIAN HOYLE

Tularemia is a plague-like disease caused by the bacterium *Francisella tularensis*. U.S. weapons stores of tularemia bacteria were reported destroyed in 1973. Until the demise of the Soviet Union, its biological weapons development program actively developed strains of the bacterium that were resistant to antibiotics and vaccines. As of March 2003, the whereabouts and disposition of some Soviet era tularemia stocks remains uncertain.

Tularemia is listed as potential bioterrorist weapon because it is easily obtained and potentially lethal.

World Health Organization (WHO) estimates hypothesize that if 50 kg of "weaponized" or highly virulent bacterium *Francisella tularensis* was dispersed in aerosol form over a large city, depending on weather and exposure patterns, there could be as many as 250,000 infections resulting in a projected 19,000 deaths.

Tularemia bacterium is transferred to humans from animals (i.e., a zoonosis) such as rodents, voles, mice, squirrels, and rabbits. Reflecting the natural origin of the disease, tularemia is also known as rabbit fever. Indeed, the rabbit is the most common source of the disease. Transfer of the bacterium via contaminated water and vegetation is possible as well.

The disease can easily spread from the environmental source to humans (although direct person-to-person contact has not been documented). This contagiousness and the high death rate among those who contract the disease made the bacterium an attractive bioweapon. Both the Japanese and Western armies experimented with *Francisella tularensis* during World War II. Experiments during and after that war established the devastating effect that aerial dispersion of the bacteria could exact on a population.

Tularemia naturally occurs over much of North America and Europe. In the United States, the disease is predominant in south-central and western states such as Missouri, Arkansas, Oklahoma, South Dakota, and Montana. The disease almost always occurs in rural regions. The animal reservoirs of the bacterium become infected typically by a bite from a blood-feeding tick, fly, or mosquito.

The causative bacterium, *Francisella tularensis* is a Gram-negative bacterium that, even though it does not form a spore, can survive for protracted periods of time in environments such as cold water, moist hay, soil, and decomposing carcasses.

The number of cases of tularemia in the world is not known, as accurate statistics have not been kept, and because illnesses attributable to the bacterium go unreported. In the United States, the number of cases used to be high. In the 1950s, thousands of people were infected each year. This number has dropped considerably, to less than 200 each year, and those who are infected now tend to be those who are exposed to the organism in its rural habitat (e.g., hunters, trappers, farmers, and butchers).

Humans can acquire the infection through breaks in the skin and mucous membranes, by ingesting contaminated water, or by inhaling the organism. An obligatory step in the establishment of an infection is the invasion of host cells. A prime target of invasion is the immune cell known as macrophages. Infections can initially become established in the lymph nodes, lungs, spleen, liver, and kidney. As these infections become more established, the microbe can spread to tissues throughout the body.

Symptoms of tularemia vary depending on the route of entry. Handling an infected animal or carcass can produce a slow-growing ulcer at the point of initial contact and swollen lymph nodes. When tularemia is inhaled, the symptoms include the sudden development of a headache with accompanying high fever, chills, body aches (particularly in the lower back) and fatigue. Ingestion of the organism produces a sore throat, abdominal pain, diarrhea, and vomiting. Other symptoms can include eye infection and the formation of skin ulcers. Some people also develop pneumonia-like chest pain. An especially severe pneumonia develops from the inhalation of one type of the organism, which is designated as *Francisella tularensis biovar tularensis* (type A). The pneumonia can progress to respiratory failure and death. The symptoms typically tend to appear three to five days after entry of the microbe into the body.

The infection responds to antibiotic treatment and recovery can be complete within a few weeks. Recovery produces a long-term immunity to re-infection. Some

people experience a lingering impairment in the ability to perform physical tasks. If left untreated, tularemia can persist for weeks, even months, and can be fatal. The severe form of tularemia can kill up to 60% of those who are infected if treatment is not given.

A vaccine is available for tularemia. To date this vaccine has been administered only to those who are routinely exposed to the bacterium (e.g., researchers). The potential risks of the vaccine, which is a weakened form of the bacterium, have been viewed as being greater than the risk of acquiring the infection.

FURTHER READING:

BOOKS:

Chin, J. "Tularemia." In *Control of Communicable Diseases Manual.* Washington, DC: American Public Health Association, 2000.

Dennis, D. T. "Tularemia." In: Wallace, R. B. ed. *Maxcy-Rosenau-Last Public Health and Preventive Medicine,* 14th edition. Stamford: Appleton & Lange, 1998.

SEE ALSO

Bioterrorism, Protective Measures
Infectious Disease, Threats to Security

Tunisian Combatant Group (TCG)

The Tunisian Combatant Group (TCG) also operates as, or is known as, the Tunisian Islamic Fighting Group.

The TCG's goals reportedly include establishing an Islamic government in Tunisia and targeting Tunisian and Western interests. Founded probably in 2000 by Tarek Maaroufi and Saifallah Ben Hassine, the group has come to be associated with al-Qaeda and other North African Islamic extremists in Europe who have been implicated in anti-U.S. terrorist plots there during 2001. In December, Belgian authorities arrested Maaroufi and charged him with providing stolen passports and fraudulent visas for those involved in the assassination of Ahmed Shah Massood, according to press reports. Tunisians associated with the TCG are part of the support network of the international Salafist movement. According to Italian authorities, TCG members there engage in false document trafficking and recruitment for Afghan training camps. Some TCG associates are suspected of planning an attack against the U.S., Algerian, and Tunisian diplomatic interests in Rome in January. Members reportedly maintain ties to the Algerian Salafist Group for Call and Combat (GSPC).

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Tupac Amaru Revolutionary Movement (MRTA)

Tupac Amaru Revolutionary Movement (MRTA) is a traditional Marxist-Leninist revolutionary movement formed in 1983 from remnants of the Movement of the Revolutionary Left, a Peruvian insurgent group active in the 1960s. The MRTA aims to establish a Marxist regime and to rid Peru of all imperialist elements (primarily U.S. and Japanese influence). Peru's counterterrorist program has diminished the group's ability to carry out terrorist attacks, and the MRTA has suffered from infighting, the imprisonment or deaths of senior leaders, and loss of leftist support. Several MRTA members remained imprisoned in Bolivia. MRTA members have previously conducted bombings, kidnappings, ambushes, and assassinations, but recent activity has fallen drastically. In December, 1996, 14 MRTA members occupied the Japanese Ambassador's residence in Lima and held 72 hostages for more than four months. Peruvian forces stormed the residence in April 1997, rescuing all but one of the remaining hostages and killing all 14 group members, including the remaining leaders. The group has not conducted a significant terrorist operation since and appears more focused on obtaining the release of imprisoned MRTA members.

MRTA is estimated to have fewer than 100 members, consisting largely of young fighters who lack leadership skills and experience. MRTA operates in Peru with supporters throughout Latin America and Western Europe.

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Turkey, Intelligence and Security

Turkey's intelligence service, MIT (Milli Istihbarat Teskilati; Special Organization) has roots that go back to the final years of the Ottoman Empire. Today, it is concerned largely with signals intelligence, and with monitoring threats from neighboring countries. Like most major industrialized nations, Turkey has a counterterrorism unit, the OIKB or National Police Jandarma Commandoes.

In 1914, Ottoman leader Enver Pasha established an intelligence service that became the Police Guild (Karakol Cemiyeti) after Turkey's defeat in World War I. In 1926, after Turkey emerged as a republic under the leadership of Ataturk (a.k.a. Mustafa Kemal), the Police Guild became MAH, the National Security Service. Directed by a former intelligence officer of imperial Germany, MAH conducted intelligence operations overseas, as well as counter-espionage work at home against Armenian and Kurdish separatists. In 1965, MAH became MIT, which has special sections devoted to internal security, counterterrorism, organized crime, Russia, Greece, Iraq, Kurdish separatists, and Cyprus.

Soldiers in OIKB are trained in aspects of riot control, hostage rescue, anti-hijacking operations, and other counterterrorism skills. Its members have conducted armed operations against Kurdish and Armenian rebels, as well as the Turkish People's Liberation Army. Controlled in peacetime by the Ministry of Interior, OIKB in wartime falls under the direction of military intelligence.

■ FURTHER READING:

BOOKS:

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

PERIODICALS:

Dempsey, Judy. "EU Military Mission at Risk from Turkish Rift." *Financial Times.* (September 19, 2002): 12.

ELECTRONIC:

Turkey: Intelligence. Federation of American Scientists. <http://www.fas.org/irp/world/turkey/index.html> (March 1, 2003).

SEE ALSO

Greece, Intelligence and Security
Syria, Intelligence and Security
NATO (North Atlantic Treaty Organization)

Turkish Hizballah

Turkish Hizballah is a Kurdish Islamic (Sunni) extremist organization that arose in the late 1980s in the Diyarbakir area in response to Kurdistan Workers' Party atrocities against Muslims in southeastern Turkey, where (Turkish) Hizballah seeks to establish an independent Islamic state. The group comprises loosely organized factions, the largest of which are Ilim, which advocates the use of violence to achieve the group's goals, and Menzil, which supports an intellectual approach. Beginning in the mid-1990s, Turkish Hizballah—which is unrelated to Lebanese Hizballah—expanded its target base and modus operandi from killing PKK militants to conducting low-level bombings against liquor stores, bordellos, and other establishments that the organization considered "anti-Islamic." In January 2000, Turkish security forces killed Huseyin Velioglu, the leader of (Turkish) Hizballah's Ilim faction, in a shootout at a safehouse in Istanbul. The incident sparked a year-long series of operations against the group throughout Turkey that resulted in the detention of some 2,000 individuals; authorities arrested several hundred of those on criminal charges. At the same time, police recovered nearly 70 bodies of Turkish and Kurdish businessmen and journalists that (Turkish) Hizballah had tortured and brutally murdered during the mid to late-1990's. The group began targeting official Turkish interests in January 2001, when 10–20 operatives participated in the assassination of the Diyarbakir police chief.

Turkish Hizballah operates primarily in southeastern Turkey—particularly the Diyarbakir region—and Turkish officials charge that the group receives at least some assistance, including training, from Iran. Turkish Hizballah strength is estimated at several hundred active members and several thousand supporters.

FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Typex

Typex was the name for the principal encryption device, or cipher machine, used by the military, intelligence, and diplomatic services of the British Empire during World War II. In the 1920s, the British were still using book cipher systems, and became aware of the need to modernize using new cipher machinery. They initially planned to use the Enigma system, but instead settled on an improved Enigma machine known as "Type X." The Typex system remained in use among British forces throughout the war.

In 1926, the British government formed an interdepartmental committee to study technology as a means of finding a replacement for the laborious system of encryption by hand. For the purposes of evaluation, the government purchased two Enigma machines, but in January 1935, the committee advised the Royal Ministry to acquire three of the "Type X" machines, which represented an improved Enigma design. Satisfied with the machine, Whitehall commissioned the Creed & Company to manufacture Type X machines to specification.

As war broke out in September 1939, the British War Office and Air Ministry had fully adopted the Typex system, although the Royal Navy would continue to perform encryption by hand until 1943. Unlike the Germans, who encrypted nearly every official message on their Enigma machines, the British used their Typex system sparingly. This may have given them an unexpected advantage, because the Germans' proliferation of enciphered messages gave the British plenty of material to study. By contrast, the Germans made no significant attempt to crack the Typex ciphers, even though they captured several of the machines at Dunkirk and in North Africa.

Britain undertook the joint development of a Combined Cipher Machine with the Americans, who developed their own Sigaba system. In 1943, the Royal Navy began using the Combined Cipher Machine. Meanwhile, the rest of the British forces continued to use Typex, though British units in the China-Burma-India theatre adopted Sigaba, while some American units adopted Typex. After the war, many Typex machines remained in use among English-speaking nations for several decades until finally, in 1973, New Zealand became the last nation to set aside its Typex system.

FURTHER READING:

BOOKS:

Freedman, Maurice. *Unravelling Enigma: Winning the Code War at Station X.* Barnsley, South Yorkshire, England: Leo Cooper, 2000.

Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two.* Frederick, MD: University Publications of America, 1984.

Melton, H. Keith. *The Ultimate Spy Book.* New York: DK Publishing, 1996.

Miller, A. Ray. *The Cryptographic Mathematics of Enigma.* Ft. Meade, MD: National Security Agency, 2001.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House,1998.

SEE ALSO

COMINT (Communications Intelligence)
Crib
Enigma
SIGINT (Signals intelligence)
Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom
Ultra, Operation

This page intentionally left blank

U

U-2 Incident

LARRY GILMAN

The U-2 spy plane, a high-altitude reconnaissance aircraft built by the U.S. starting in the 1950s, was the subject of many "incidents" or diplomatic confrontations with the Soviet Union during the Cold War; however, the debacle referred to as *the* U-2 incident began on May 1, 1960, when a U-2 plane flown by Central Intelligence Agency (CIA) pilot Gary Powers took off from a U.S. air base at Peshawar, Turkey. The mission scheduled for Powers, codenamed Grand Slam, was to be the most ambitious U-2 flight undertaken up to that time. Its route would take it from Turkey to Soviet nuclear-weapons facilities in the Ural Mountains, various railroads, intercontinental ballistic missile sites in Siberia, then back across northern Russia, there to photograph shipyards before leaving Soviet airspace above the Arctic Circle and landing in Bodo, Norway.

The mission was unsuccessful. Powers took off at 6:26 A.M. on what was to have been the twenty-fourth U-2 overflight of the Soviet Union. He flew first to the east, over Iran to Afghanistan, in order to cross the Soviet border from an unexpected direction. He was, however, detected by Soviet radar while still 15 miles from the Afghan-Soviet border. Although undesirable, detection was not unusual; in fact, all previous U-2 flights over the Soviet Union had been detected at some point. The U-2 relied for success not primarily on stealth but on the fact that the Soviets had no fighter planes or, for the first few years, surface-to-air missiles that could fly high enough (70,000 ft [21 km]) to shoot it down. A recently deployed Soviet surface-to-air missile, the SA-2, could reach the U-2, but only if it happened to be stationed in the plane's flight-path and if its operators were on alert status, ready to fire.

Powers flew over an SA-2 battalion soon after entering Soviet airspace, but its crew was not on alert and so could not fire while he was within range. About a dozen Soviet MiG fighter planes also attempted to shoot down Powers's U-2, but could not climb high enough to get within weapons range.

Soviet premier Nikita Khrushchev (1894–1971) was notified of Powers's ongoing flight at 8:00 A.M. Moscow time. It being May 1 (May Day or International Labor Day), he was preparing for the massive official festivities that always scheduled for that occasion. Outraged at what he perceived as a deliberate political provocation, he ordered that Powers's U-2 be shot down at any cost.

By this time Powers was approaching the Russian city of Sverdlosk. The pilot of an Su-9 fighter jet was ordered to carry out a suicide attack on Powers, ramming the U-2 with his own plane; however, he was unable to locate Powers. An SA-2 battalion stationed outside the city was on alert, and when Powers entered its zone of engagement it fired a missile. It exploded near Powers's plane. The fragile U-2 was damaged by the concussion and began to break to pieces. Powers managed to bail out, and was captured as soon as he parachuted to the ground.

Because the U-2 overflights violated treaty law, the U.S. always denied publicly that they were occurring. Early on, in fact, the CIA, which ran the U-2 program, had considered using non-U.S.-citizens as pilots. Therefore, after the loss of Powers's plane (but before the Soviet Union had revealed that it had captured Powers alive) the U.S. issued several false cover stories. The National Aeronautics and Space Administration (NASA), for example, claimed that it had lost a U-2 being used as a weather plane over Turkey; the idea was that if the Soviets recovered the plane itself, the U.S. would claim that it had strayed accidentally into Soviet airspace when its oxygen supply failed and the pilot lost consciousness. A spokesman for the U.S. Department of State assured reporters at a press conference in Washington, D.C., on May 6 that "There was no—N-O—no deliberate attempt to violate Soviet air space, and there has never been," and added that it was "monstrous" of the Soviets to assert that the U.S. would lie to the world.

But the next day, May 7, Khrushchev revealed that he had proof that the U-2 had been a spy plane: Powers himself. The statements by NASA and the State Department were exposed, causing an international political embarrassment for the U.S. On May 11, President Eisenhower made a speech in which he admitted that the U.S. had been overflying the Soviet Union. That same day, the remnants of Powers's U-2 were put on public display in Gorky Park in Moscow and were toured by Soviet leaders. Political protest in Japan caused the U.S. to withdraw its U-2 detachments from that country; soon the U.S. had withdrawn all its other overseas U-2 detachments as well. For the U.S., both the political and operational costs of the U-2 incident were high.

Powers was questioned, but revealed nothing of value to his captors. He was sentenced to 10 years in prison as a spy but was traded back to the U.S. for a captured Soviet spy two years later. Coincidentally, the day Powers was sentenced—August 19, 1960—the U.S. made its first use of a technology that would eliminate altogether the need for U-2 overflights of the Soviet Union, recovering a film package from its first spy satellite, the Corona. The Corona's pictures showed more of the Soviet Union (albeit at lower resolution) than all reconnaissance missions made up to that time by the U-2 and high-altitude balloons. From that day forward satellites, not airplanes, would provide direct intelligence of Soviet activity—and would do so without political risk.

FURTHER READING:

BOOKS:

Peebles, Curtis. *Shadow Flights: America's Secret Air War against the Soviet Union.* Novato, CA: Presidio. 2000.

SEE ALSO

U-2 Spy Plane

U-2 Spy Plane

LARRY GILMAN

The U-2 is a jet-powered reconnaissance aircraft specially designed to fly at high altitudes (i.e., above 70,000 ft [21 km]). It was used during the late 1950s to overfly the Soviet Union, China, the Middle East, and Cuba; flights over the Soviet Union, the primary mission for which the plane was designed, ended in 1960 when a U-2 flown by CIA pilot Gary Powers was shot down over the Soviet Union. This event was a major political embarrassment for the U.S. A redesigned version of the U-2, the U-2R, was used from the late 1960s through the 1990s. The U-2R was used extensively during the Gulf War of 1991, for example, to monitor Iraqi military activities. A more recent version of the U-2, the U-2S, is deployed today. The U-2S has been used recently by both the United States and United Nations weapons inspectors to make observations of North Korea and Iraq.

Background. Shortly after the end of World War II, the tenuous alliance between the Soviet Union, the United States, and the nations of Western Europe ruptured. The Soviets took control of Eastern Europe, the North Atlantic Treaty Organization (NATO) was formed by the U.S. and its European allies, and the Cold War began in earnest. Tensions were high, and war between NATO and the Soviet Union often seemed imminent. Military planners desired what they termed "pre-D-day intelligence" about the Soviet order of battle, that is, information about the Soviet military obtained before a war began. Spy satellites would not become available until the early 1960s, leaving aircraft as the primary means of obtaining up-to-date information about Soviet military and industrial activities.

A number of photographic spy overflights of Eastern Europe, the Soviet Far East, China, and the periphery of the Soviet Union were made in the late 1940s and early 1950s using various U.S. and British aircraft including the RB-29 bomber, the B-47B bomber, the RF-80A fighter (the first operational U.S. jet fighter), the RF-86F fighter, and the RB-45C reconnaissance aircraft. None of these planes had enough range to penetrate very far into Russia itself, where nuclear testing grounds and missile bases were located; nor could they fly at altitudes high enough to avoid interception by Soviet MiG jet fighters.

By the mid-1950s, Soviet air defenses had improved to the point where overflights by available aircraft had become impractical. Development of a lightweight, high-altitude, single-pilot plane (originally dubbed the CL-282 but later the U-2, a deliberately misleading designation suggesting a "utility" aircraft) began in 1954. However, the plane could not ready until 1956; in the meantime, high-altitude, unmanned balloons were used to carry camera packages over the Soviet Union. These balloons, codenamed Genetrix balloons, were launched in Norway, Scotland, Turkey, and West Germany, from whence they were carried by global tradewinds across the Soviet Union to recovery zones over the Pacific Ocean. Some 379 Genetrix balloons entered Soviet airspace in 1955 and 1956; 235 were shot down by MiGs or antiaircraft guns, and only 44 were recovered. The success rate would have been higher except that President Dwight Eisenhower had ordered that the balloons not fly at their true maximum altitude (70,000 ft [21 km]); he reasoned that if the balloons were restricted to an altitude ceiling of 55,000 ft (17 km), where the Soviets could shoot them down most of the time, the Soviets would not be motivated to develop high-altitude interceptors that could be later used against the U-2.

Gary Powers, shown while an Air Force Reserve pilot, later flew an American U-2 spy plane over Russia in 1960 and was shot down, held prisoner, was subjected to a public show-trial, and ultimately returned to the West in exchange for a Russian spy. AP/WIDE WORLD PHOTOS.

Design. The U-2 is built much like a glider, with ultralight construction and long, narrow wings that measure 80 ft (24 m) from tip to tip, longer than the plane itself. (The U-2C, first flown in 1978, has a wingspan of 103 ft [31 m].) Wings of this type, mounted at right angles to the body of an aircraft, provide high lift (i.e., upward aerodynamic force resulting from airflow around the wing); this is necessary at 70,000 ft because the atmosphere is so thin. The U-2's cruising altitude takes it so close to outer space that the sky above appears black and the curvature of the Earth is visible.

The U-2 had other features intended to reduce its weight and thus increase its cruising altitude and range. The wings were bolted to the body of the aircraft rather than supported, as in standard jet aircraft of that period, by a spar running right through the fuselage. The tail assembly was held on by only three bolts; the skin of the fuselage was thin aluminum; flight controls were manually powered, so the pilot flew the plane by muscle power; and there was no radar. In-line "bicycle"-type landing gear was employed, consisting of a main unit under the plane's nose and small wheel at the tail; upon landing, the U-2 would taxi to a halt and then tip over onto one wing. For takeoff, small detachable supports or "pogos" held the wings off the ground and were dropped when the plane was airborne.

A camera package termed the A-2 was installed in the aircraft's belly; it contained three still cameras, one pointing straight down and the other two pointing to the left and right of the aircraft's direction of travel, as well as a tracking camera that filmed a continuous record of the plane's mission.

Development of the U-2 and of reconnaissance balloons required numerous test flights over the United States. The balloons were often visible from the ground as metallic-looking ellipses, and prototype U-2 planes were sometimes spotted from civilian airliners; these sightings giving rise to many reports of unidentified flying objects (though to be alien spacecraft). Because the devices actually causing the sightings were secret, the government offered often uncreditable explanations for the sightings, inadvertently helping to encourage bizarre UFO beliefs.

Because of the need to fly light, the U-2 does not carry weapons. Nor can it undertake evasive maneuvers if fired upon, for it is delicate, and breaks up if subjected to strong forces. It is designed to fly high and far.

Deployment. On June 20, 1956, the first U-2 flight over a "denied area"—Warsaw Pact airspace—was made. The flight passed over Czechoslovakia, Poland, and East Germany. On July 1956, flights over the Soviet Union itself commenced, with a flight over Leningrad to photograph the shipyards. MiG fighters attempted to intercept the U-2, which was detected by Soviet radars, but were unable to attain its altitude. The next day a U-2 overflew Moscow itself, photographing the Kliningrad missile factory and Khimki rocket-engine factory north of the city.

Although the U.S. did not officially admit the existence of the U-2 flights, due to Soviet diplomatic protests President Eisenhower ordered all U-2 overflights of the Soviet Union temporarily suspended late in 1956. U-2s were used during this interval to spy on French and British actions in the Middle East during the Suez Crisis. Eisenhower ordered U-2 flights resumed after the Soviets crushed the Hungarian rebellion of October 1956. This Soviet aggression heightened tensions between NATO and the Warsaw Pact and increased the U.S. desire for intelligence data. Over the next few years, the U-2 was flown over China and Vietnam as well the Middle East, Eastern Europe, and the Soviet Union.

On May 1, 1960, a U-2 was shot down over Russia by a surface-to-air missile. The pilot was captured, tried for espionage, and sentenced to 10 years in prison. (He was traded for a captured Soviet spy two years later.) No more overflights of the Soviet Union were attempted. Coincidentally, however, the U.S. spy satellite program accomplished its first recovery of a film packet from space on the day that Powers was sentenced (August 19, 1960). The U-2 was, therefore, no longer a unique source of intelligence about affairs inside Soviet territory. However, it still had an important role to play in military history. On October 14, 1962, a U-2 flying over Cuba took pictures that proved that the Soviet Union had established sites for launching medium-range ballistic missiles in Cuba. The presence of these nuclear-armed missiles in Cuba, combined with U.S. insistence that they be removed, gave rise to the Cuban Missile Crisis, which almost resulted in war between the U.S. and Soviet Union in October 1962.

Despite radical improvements in spy satellite capabilities since the 1960s, U-2 planes continue to provide some intelligence data. Some experts believe that U-2S photographs of North Korean facilities were the basis of the U.S. discovery in October 2002 that North Korea was producing enriched uranium for nuclear weapons. In 2003, proposed U-2S overflights of Iraq to support United Nations weapons inspections were a subject of controversy between the U.S. and Iraq. Furthermore, a civilian version of the U-2, the ER-2, is used by the U.S. National Aeronautics and Space Administration for Earth-resources research. The ER-2 has even made flights over Russia—with official permission.

■ FURTHER READING:

BOOKS:

Peebles, Curtis. *Shadow Flights: America's Secret Air War against the Soviet Union.* Novato, CA: Presidio, 2000.

SEE ALSO

U-2 Incident

Ukraine, Intelligence and Security

Much of Ukraine's intelligence and special operations structure bears the imprint of the nation's Soviet past. Both the Security Service of Ukraine (Sluzhba Bespeky Ukrayiny; SBU) and its principal action unit are based on Soviet models. Internationally, the Ukraine has come under suspicion as a supplier of materials to rogue states and groups.

Founded in 1991, the SBU took over the old KGB Ukrainian headquarters in the capital city of Kiev. It also took on the organization structure, in many cases the tactics, and even many of the personnel of its Soviet predecessor. Like KGB, it oversees both security and intelligence operations, and through its subunit GUR, fights organized crime, terrorism, drug trafficking, and arms smuggling. Another important SBU subunit is the action group Administration A, the "Alpha" unit. Named and modeled after the Soviet Alpha unit that attacked the presidential palace in Kabul in 1979, setting off the Soviet-Afghan war, it has counterterrorism and witness protection responsibilities.

Despite its stated opposition to terrorism, Ukraine has been accused to supplying materiel to terrorist states and groups. Not only did it supply two helicopters to Slobodan Milosevic's Serbia in 1999, but in 2002, it was under investigation by United States and British arms experts on allegations that it had sold sophisticated Kolchuga radar systems to Iraq. Ukraine has also been accused, along with Russia and the regime of President Aleksandr Lukashenko in Belarus, of selling weapons to rebel armies in Sierra Leone and Liberia. Western intelligence sources also reported that representatives of Afghanistan's Taliban regime and the Muslim terrorist network al-Qaeda visited Kiev in September 1999, looking to purchase arms, parts, and training.

■ FURTHER READING:

BOOKS:

Anderson, Robert. "The Former Soviet Republics Are Accused of Supplying Weapons to Rogue States in Defiance of United Nation or U.S. Embargoes." *Financial Times* (October 21, 2002): 27.

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Kuzio, Taras. "Details Emerge on Kiev's 'Alpha' Unit." *Jane's Intelligence Review* 11, no. 10 (October 1, 1999): 1.

Warner, Tom. "U.S. Plans to Shun Ukraine President over Radar." *Financial Times* (November 9, 2002): 10.

ELECTRONIC:

Ukraine Intelligence. Federation of American Scientists. <http://www.fas.org/irp/world/ukraine/> (March 1, 2003).

SEE ALSO

*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
Russia, Intelligence and Security

Ulster Defense Association/ Ulster Freedom Fighters (UDA/UVF)

The Ulster Defense Association/Ulster Freedom Fighters (UDA/UVF) is the largest loyalist paramilitary group in Northern Ireland, and was formed in 1971 as an umbrella organization for loyalist paramilitary groups. It remained a legal organization until 1992, when the British Government proscribed it. Among its members are Johnny Adair, the only person ever convicted of directing terrorism in Northern Ireland, and Michael Stone, who killed three people in a gun and grenade attack at an IRA funeral. The UDA joined the UVF in declaring a cease-fire in 1994, which broke down in January 1998, but was later restored. In October 2001, the British Government ruled that the UDA had broken its cease-fire. The organization's political wing, the Ulster Democratic Party, was dissolved in November 2001. The group has been linked to pipe bombings and sporadic assaults on Catholics in Northern Ireland; where it stepped up attacks in 2001. William Stobie, the group's former quartermaster who admitted to passing information about the UDA to the British government, was murdered in December 2001; the Red Hand Defenders claimed responsibility for the killing.

Estimates of UDA strength vary from 2,000 to 5,000 members, with several hundred active in paramilitary operations throughout Northern Ireland.

■ FURTHER READING:

ELECTRONIC:

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001," Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

Ultra, Operation

ADRIENNE WILMOTH LERNER

Operation Ultra was the codename for the British cryptologists efforts at Bletchley Park to intercept and break German coded messages. While Ultra initially was the cryptonym for the project to break the German Enigma machine, the code name came to represent all British efforts to break high-level German radio codes during World War II.

Bletchley Park and Operation Ultra

Surveillance of high-level German communications began at Bletchley Park in 1938. Thirty code breakers, linguists, mathematicians and other experts formed the first class of the new government cipher school. Within a year, British military intelligence employed over 500 people at Bletchley Park. The cryptology team had several early successes breaking lower-level German government intercepts that used mathematical and word replacement codes. However, a complex, machine-produced mathematical cipher, appeared in the wire traffic. British codebreakers nicknamed the foreign cipher machine Enigma. As tensions in Europe escalated, and war seemed imminent, Enigma intercepts increased from a few to a few hundred a day. In 1939, Operation Ultra charged cryptologists with breaking the Enigma code and devising a rapid means of transcribing the intercepts.

The breaking of Enigma began even before the creation of the Bletchley Park cryptanalysis department. Polish intelligence began monitoring German communications and breaking their codes in the mid-1930s. However, the Germans created a new cipher, Enigma, in the summer of 1938. When Britain and France pledged their support to ensure Poland's freedom from invasion and domination by Nazi Germany, Polish intelligence shared all of their code-breaking information and technology with Britain and France. Defying the Munich Agreement, Germany invaded Poland in 1939, beginning World War II.

British cryptologists decoded German communications with limited success in the early months of the war. Some codes were broken mathematically and then decoded in long hand, an arduous process. Other codes, mainly used for low-level security communications used decades-old codes broken by French, British, Polish, or Swedish intelligence. In 1940, mathematicians at Bletchley Park broke the German Enigma machine. Modifying plans given to them by the Poles, Ultra engineers constructed a bombe, a code-breaking machine, to aid in deciphering Enigma intercepts. Naval WRENs, members of the Royal Navy women's corps, operated the noisy, large, and cumbersome bombes. Throughout the war, women on staff at Bletchley Park outnumbered men eight to one.

Gathering coded data and intercepting German messages was almost as grueling a task as deciphering the communications. British military signals and radio specialists staffed thousands of "Y" intercept stations on the coast and in Europe. Transmissions were affected by weather phenomena, interference from jamming machines, background noise, and congested airwaves. Thus, intercepted data was often difficult to understand. The German government and military used over 200 frequencies to broadcast messages, most of which lasted less than 30 seconds. Coded wire traffic was often broken off in mid course or sent over new. Wires known to be tapped were constantly replaced. What communications data was collected at the stations was then sent to Bletchley Park cryptologists and translators, either by courier or coded teleprinter.

Ultra staff and technology successfully decoded over 50 messages a week. However, by 1942, German radio and wire traffic increased exponentially. The 1,200 member staff of Bletchley Park could not efficiently decipher the thousands of intercepts received daily. Even the construction of more bombes did not significantly aid progress on Ultra. Since the decoding, translating, and transcription process was slow, the intelligence gathered from intercepts could not be used to its full potential. When British cryptologists broke the more complicated German *Geheimschreiber* cipher machine, Ultra intelligence nearly doubled.

Engineers Alan Turing and Tommy Flowers devised a complex machine to decipher and transcribe German intercepts. The device, appropriately nicknamed Colossus, could handle the thousands of intercepts arriving daily at Bletchley Park. The massive task of transcribing and photographing decoded messages for storage in the archives was greatly reduced since Colossus transcribed the messages, in the original German, directly on to a typewriter. Colossus proved so efficient that British intelligence soon learned it could decipher messages more rapidly than could the intended recipients. Ultra intelligence became a key part of British battle strategy, giving British military command advance information on German military operations.

Secrecy and security. Worried that the German military and government would change encryption devices if they knew

of the operation, Ultra was shrouded in absolute secrecy. For security, the details of the entire Operation Ultra were fully known by only four people, only one of whom routinely worked at Bletchley Park. Dissemination of Ultra information did not follow usual intelligence protocol, but maintained its own communications channels. Military intelligence officers gave intercepts to Ultra liaisons, who in turn forwarded to the intercepts to Bletchley Park. Information from decoded messages was then passed back to military leaders through the same channels. Thus, each link in the communications chain knew only one particular job, and not the overall details of Ultra.

The massive archives of intercepts decoded at Bletchley Park were reproduced in entirety. A photograph of each intercept, and its English translation, were archived at the Bodleian Library at Oxford University in case German forces located and bombed the Bletchley Park complex. A train was on constant reserve at nearby Bletchley Station to ferry code breaking records and equipment to Liverpool, from where it would be shipped to American intelligence headquarters in the event of a German invasion.

Within Britain, the Ultra secret was closely guarded. However, British intelligence did share cryptological advances, including information on Ultra and the Enigma machine, with the American and French intelligence community. Joint American-British information exchanges became more commonplace. American intelligence shared information on Magic, their code-breaking operation against Japan. In the months before Pearl Harbor, a group of American cryptologists was sent to Bletchley Park to observe British code-breaking operations. Information provided by Bletchley Park aided American cryptologists in breaking the Japanese Purple machine. Germany shared their encryption technology with its Japanese allies. As was the case with Enigma, Allied cryptologists broke the Purple machine but the Japanese continued to use its code throughout the war. American code-breakers also worked on German codes and the design of decoding machines. The American department working on German codes also called itself Ultra.

While the British shared details of Ultra with American and French intelligence, the project was kept secret from the Soviet Union, despite the Soviets' status as wartime allies. Soviet intelligence knew of Bletchley Park, but the British kept the fact that cryptologists broke the Enigma code secret. Information from important messages containing German battle plans and troop positions was disguised as intelligence gathered from Resistance groups in France and Switzerland. Soviet military intelligence believed the information originated from operatives in the Communist spy network, Sandor Rado.

Ultra intelligence and the Allied war effort. Operation Ultra's major shortcoming was that intelligence dispatches were not processed quickly enough in the early war years to aid in the Battle of Britain, and spare London the full force of the Blitz. German U-boats dominated the seas, and Allied fighter commands had little reliable intelligence information until 1942.

With the invention of Colossus, a secure and reliable network through which to disseminate information, and the tireless work of the Bletchley Park staff, Ultra information was successfully used in several pivotal Allied military operations. Monitoring German naval dispatches, code-breakers determined fleet positions, allowing convoys to divert their routes and safely cross the Atlantic. German U-boats lost their strategic element of surprise, and Allied forces located and sank the German submarines with increasing frequency. One of the great victories and British morale boosters during the war was the sinking of the German destroyer *The Bismarck*.

While the guarantee of safe passage for Allied supply ships was important in the Atlantic, it was vital in the smaller waters of the Mediterranean Sea. Ultra intercepts noted that the Germans anticipated an assault on Sicily. Allied forces postponed their invasion until they convinced German forces they intended to invade the Balkans and Greece. False communications sent via a British-built Enigma machine added to the ruse, and the German army redeployed troops to the Balkans. Ultra intercepts confirmed the revised German troop positions, and the Allies then continued with their planned invasion of Sicily and Italy.

Ultra information regarding Hitler's "Atlantic Wall" defenses in France helped Allied forces plan the D-Day invasion. Ultra intercepts yielded information that German high command thought that an Allied invasion of France, it if occurred, would most likely take place on the beaches near Pas de Calais. The British planted false information for German intelligence, the *Abwehr,* to confirm their suspicions. The Germans diverted a significant number of troops to the area, lessening the defenses on the northern Normandy beaches where the Allied invasion landed. As Allied troops progressed through France, commanding officers received daily Ultra intelligence updates.

The closely guarded secret of Ultra was never discovered by the Axis powers. Germany continued to use Enigma throughout the war, giving the Allies a decided tactical advantage and nearly eliminating the element of surprise in German offensives. After the war, the cryptology department at Bletchley Park was disassembled, the archives removed to classified storage, and the complex deciphering equipment destroyed. The veil of secrecy extended to the wartime staff of Bletchley Park, none of whom disclosed information about Ultra until the project was officially declassified in 1989. Bletchley Park secrets were so closely guarded that one of the major accomplishments of Operation Ultra was slighted its deserved historical recognition. The electronic, programmable Colossus, with its 2,500 tubes, predated the American ENIAC machine, widely regarded as the world's first computer, by two years.

FURTHER READING:

BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War.* Cambridge: Cambridge University Press, 1988.

Hinsley, F. H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park.* Oxford: Oxford University Press, 2001.

Stinson, Douglas. *Cryptography: Theory and Practice*, second edition. Chapman and Hall, 2002.

SEE ALSO

Bombe
Codes and Ciphers
Codes, Fast and Scalable Scientific Computation
Colossus I
FISH (German Geheimschreiber *Cipher Machine*
Operation Magic
Purple Machine
World War II, United States Breaking of Japanese Naval Codes

Ultrashort-Pulse Laser Technology.

SEE *Lawrence Livermore National Laboratory (LLNL).*

Underground Facilities, Geologic and Structural Considerations in the Construction

WILLIAM C. HANEBERG

Natural and manmade underground facilities have played an important role in warfare and national security for more than 5000 years. Underground chambers were used for hiding places and escape routes in Mesopotamia and Egypt from 3500 to 3000 B.C., and they continue to play an important role in the ongoing conflict in Afghanistan. Some notable twentieth-century uses of underground facilities for warfare and national security include dozens of underground factories constructed beneath Germany during World War II; the Cheyenne Mountain Operations Center, Colorado; as many as 1000 underground facilities estimated to exist beneath the Korean Demilitarized Zone; and countless natural and manmade caves used by al-Qaeda forces in Afghanistan. Large manmade cavities in salt domes along the Gulf Coast, some of them larger than 17 million cubic meters in volume, are used for the United States Strategic Petroleum Reserve. The details of underground facilities used for military or national security purposes are classified, but there is no reason to assume that they are not on the scale of underground civil projects. The largest unsupported span ever constructed in rock was a 61 m (200 ft) wide hockey arena constructed for the 1994 Winter Olympics in Norway, and underground mines in many parts of the world consist of smaller passages that extend for many miles.

Extensive underground facilities have also been constructed to maintain communications and house the United States government in the event of an attack. An underground facility known as Site R exists within Raven Mountain, Pennsylvania, and is thought to have been the location from which Vice President Cheney and other officials worked in the aftermath of the September 11, 2001 terrorist attacks. Construction of Site R was authorized by President Truman and completed during the early 1950s. Declassified information dating from the construction period describes a three-story underground facility with more than 18,000 square meters of floor space and room for more than 5000 people. The existence of another extensive underground facility beneath the Greenbrier Resort in West Virginia, constructed to house the United States Congress in the event of a nuclear attack, was made public in 1992.

Although they can be expensive and difficult to construct, underground facilities offer two important advantages over surface structures. First, they are almost completely hidden from view and activities within them can be invisible to even the most sophisticated intelligence satellites. Second, their depth can make them resistant to conventional and some nuclear attacks. Additional advantages include lower long-term maintenance costs (because underground structures are not exposed to weather) and lower heating and cooling costs (because temperature is constant in underground environments). The detection and characterization of underground facilities and the development of technologies to defeat hardened underground facilities are among the principal goals of modern military geologists.

Geologic factors exert an important influence on the design and construction of any underground facility. One of the most important factors is the strength of the soil or rock into which underground structures are excavated. Shallow underground structures can be constructed in soil or highly weathered rock using a technique known as cut-and-cover construction. These structures are built by first excavating a hole, then building the desired facilities, and finally covering the completed structures with soil. Because soil and weathered rock near Earth's surface tends to be weak, shallow cut-and-cover structures must be heavily reinforced with concrete or other materials if they are to withstand attack. The mineral quartz, which can be a common component of the rocks that are used for concrete aggregate, changes volume when it undergoes a phase transition at high temperatures (844 degrees K at a

A car enters the U1a Complex, an underground facility in Nevada designed for conducting subcritical experiments to determine whether aging nuclear weapons remain reliable and safe. AP/WIDE WORLD PHOTOS.

pressure of 0.1 MPa). In order to prevent thermal disintegration, therefore, aggregate for concrete that may be subjected to extremely high temperatures must consist of rocks containing little quartz. Cut-and-cover structures can be difficult to hide during construction, when they can be easily pinpointed on remote sensing images or aerial photographs. It may also be possible to locate shallow cut-and-cover structures after construction if soil disruption or activity within the structure produces a thermal, soil moisture, or soil chemistry anomaly identifiable through multispectral or hyperspectral image analysis.

Deep underground facilities can be constructed using specialized tunnel boring machines (TBMs) or by underground drilling and blasting. These construction techniques are used extensively in the underground mining industry and the construction of civil works such as tunnels. Tunnel boring machines are large pieces of construction equipment with faces that consist of rotating cutting tools, allowing the machine to drill itself into earth or rock and create tunnels many meters in diameter. Underground construction by drilling and blasting begins with a carefully designed pattern of holes drilled into a rock face. The holes are loaded with explosive charges that are detonated according to a specified sequence in order to efficiently fracture and loosen the rock, which is then removed to expand the underground opening.

The primary geologic factor controlling underground construction in rock is the nature of the rock itself. Strong rock with uniform physical properties is the preferred choice for underground construction. Clandestine tunnels excavated beneath the Korean Demilitarized zone by North Korea, for example, tend to be located in granite that is relatively uniform and contains few fractures rather than adjacent rocks that are more highly fractured. Depending on the geologic setting of an underground facility, selecting choice rock may not be an option. Rocks are commonly heterogeneous, with physical properties such as strength and degree of natural fracturing varying from place to place.

Engineering geologists and civil engineers commonly describe the physical quality of rock using a simple parameter known as the Rock Quality Designation, or RQD, which is obtained by measuring core samples obtained during exploratory drilling prior to construction. The RQD is the percentage of pieces of core sample longer than 10 cm (4 in) divided by the total length of core. Thus, a core sample of intact rock with no fractures or cracks would have an RQD of 100. A core sample of highly fractured rock in which only one-quarter of the pieces are longer than 10 cm would have an RQD of 25. Other factors that affect the design and construction of underground facilities in rock include the number and density of natural fractures in the rock, the roughness of fracture surfaces and the degree of natural chemical alteration along fracture surfaces (both of which affect rock strength), the presence or absence of water in the fractures, and the presence or absence of zones of weakness such as faults or rock that has been altered to the consistency of clay. Highly fractured rock near a large fault, for example, may be too weak to support itself above an underground cavity or serve as a conduit for high-pressure water that can quickly flood an underground opening. Completion of the NORAD underground facility in Cheyenne Mountain during the 1960s, for example, was delayed for more than a year because of problems with a geologic fault intersecting the ceiling of the

underground opening. Underground openings in weak, highly fractured, or water saturated rock can be lined with reinforced concrete or shored with steel beams in order to ensure the safety of construction workers and later occupants of the space. The lithostatic stress that must be resisted by underground openings of any size increases linearly with depth, and the most stable underground openings are generally circular or spherical. Rectangular or cubic openings contain sharp corners that concentrate stresses in the rock and can lead to the collapse of the opening.

One issue that is important for military or security-related underground facilities, but generally not for civil structures, is their vulnerability to attack by conventional or nuclear weapons. The vulnerability of an underground facility to a conventional weapon attack is a function of its depth, the strength of the overlying rock, and the penetrability of the soil or rock exposed on Earth's surface above the facility. Knowledge of these properties is essential to those designing facilities to survive attacks as well as to those designing specialized earth penetrating weapons (EPWs). The geologic information necessary to evaluate the vulnerability of a facility has been given the name "strategic geologic intelligence" by some military geologists. Few, if any, underground facilities can withstand a direct nuclear attack.

FURTHER READING:

BOOKS:

Underwood, J. R., Jr. and P. L. Guth, editors. *Military Geology in War and Peace.* Boulder, Colorado: Geological Society of America, 1998 .

PERIODICALS:

Weiser, Carl. "'Secret' Government Site Not So Secret after All." *USA Today* (June 26, 2002).

ELECTRONIC:

Leith, William. "Military Geology in a Changing World." Geotimes, American Geological Institute. February 2002. <http://www.agiweb.org/geotimes/feb02/feature_military.html>(December 10 2002).

Linger, D.A., G.H. Baker, and R.G. Little. "Applications of Underground Structures for the Physical Protection of Critical Infrastructure." CE World. 2002. <http://www.ceworld.org/ceworld/Presentations/CriticalInfrastructure/Applications-of-Underground-Structures-for-the.cfm> (December 11 2002).

"Rock Tunnelling Quality Index." Edumine. <http://www.edumine.com/Xtoolkit/tables/rtqitables.htm>(December 11 2002).

U.S. Air Force. "Cheyenne Mountain Operations Center." <https://www.cheyennemountain.af.mil/cmocindex.html>(December 11 2002).

SEE ALSO

Architecture and Structural Security
Continuity of Government, United States
Geologic and Topographical Influences on Military and Intelligence Operations
Hardening
Vulnerability Assessments

Undersea Espionage: Nuclear vs. Fast Attack Subs

JUDSON KNIGHT

In developing its submarines, the United States has tended to pursue technical, rather than numerical, superiority. Such was the case during the Cold War, when the United States led in nuclear submarine development while the Soviets marshaled a much larger submarine fleet. After the Cold War concluded, Washington was faced with the possible threat of non-nuclear submarine deployment by third world nations.

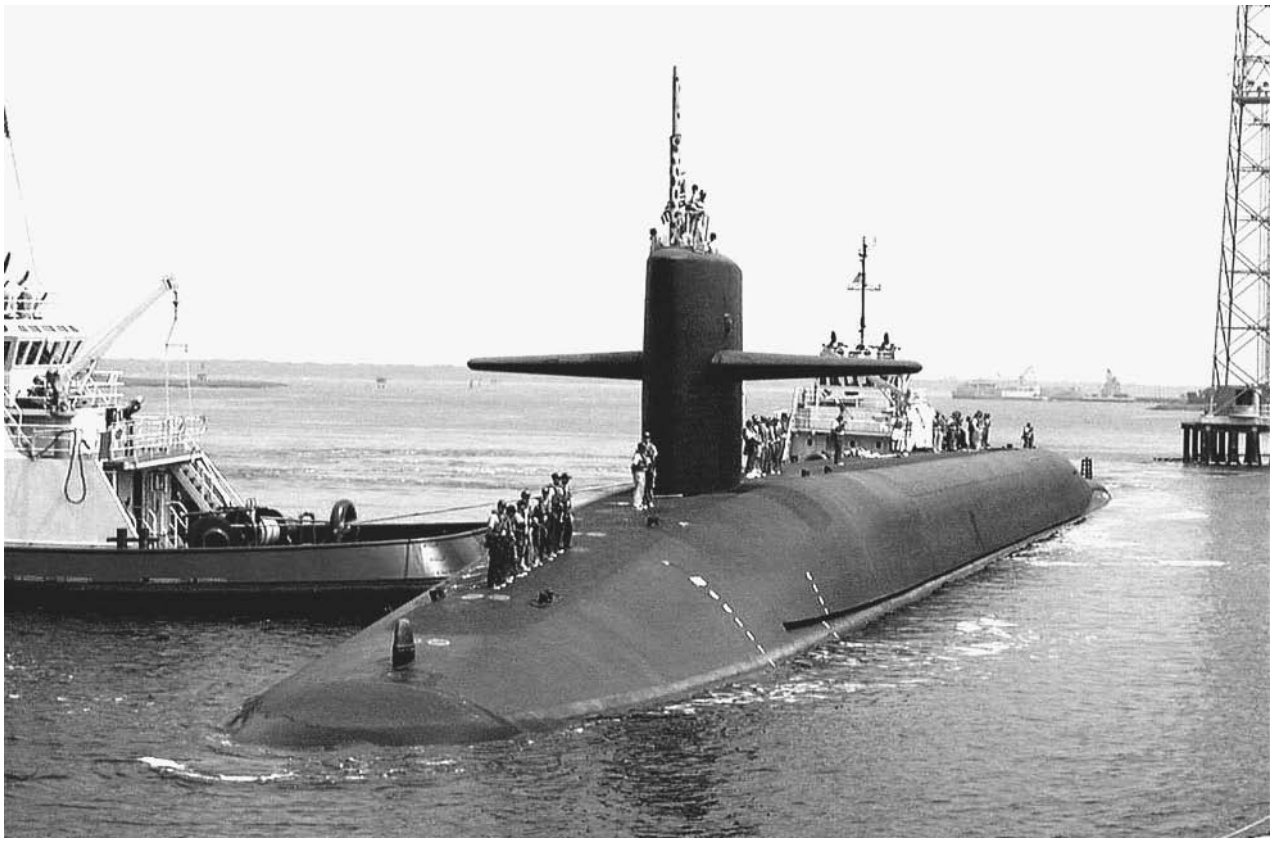
U.S. Submarines

During the Cold War, there were two principal types of U.S. submarines, the fast attack submarine (SSN) and the nuclear-powered ballistic missile submarine (SSBN), nicknamed the "boomer." Both were nuclear-powered.

Fast attack submarines were tasked toward locating and tracking their Soviet counterparts, for which they carried extensive intelligence-gathering equipment. Their principal weapon was the torpedo, although at times they were armed with tactical missiles such as the cruise missile. The U.S. Navy's first nuclear sub was the *Nautilus,* commissioned on September 30, 1954. It was followed during the 1950s by almost two dozen other craft, including several in the Skate, Shipjack, and Triton classes.

Sturgeon and Los Angeles classes. The Navy inaugurated a new era with the commissioning of the *Sturgeon* on March 3, 1967. First in a 37-member class, the *Sturgeon* was powered by a single Westinghouse Model 5 pressurized-water nuclear reactor. Its speed was an impressive 20 knots (37 kph) on the surface and 25 knots (46 kph) when submerged. (These figures are approximate, since the exact speed of the *Sturgeon* class is classified.)

Another phase in this second generation of SSNs was the Los Angeles class, a group of 62 craft that can submerge to depths of 800 feet (240 m) or more. At 362 feet (110 m) long and 33 feet (10 m) abeam, they can accommodate a crew of 127 or more. The Los Angeles class was



The USS *Louisiana*, an Ohio-class nuclear powered submarine with an armament including 24 Trident II missiles, arrivies at its home port in King's Bay, Georgia. AP/WIDE WORLD PHOTOS.

built during a period from the mid-1970s to the mid-1990s, and many are still in use.

"Boomers" and beyond. During the period from 1960 to 1966, the Navy introduced a total of 41 SSBNs, or "boomers." This group was nicknamed "41 for Freedom," because each was named after a hero from American history, as reflected in the names of the three classes: George Washington, Ethan Allen, and Benjamin Franklin. (The first two groups consisted of five submarines each, with 31 in the third group.) Each of these carried 16 Polaris nuclear missiles, but in 1972, conversion to the more accurate Poseidon missile began. By 1979, the even more advanced Trident I missile had been introduced, and the last 12 of the original 41 SSBNs were converted for this missile.

The next generation of SSBN arrived with the *Ohio,* which inaugurated a much larger class of sub in 1981. Ohio class subs are 560 feet (170.7 m) long and 42 feet (12.8 m) abeam. The first 12 were equipped to carry 24 Trident I missiles, and with the introduction of the Trident II in 1990, subsequent models were built for this newer, larger missile. The 18 SSBNs of the Ohio class together carry 50% of all U.S. strategic warheads.

Four of the Ohio class were scheduled for inactivation in 2003 and 2004, but instead they are being converted to guided missile submarines (SSGN). The primary mission of the latter will be support for land attack and special operations forces, a change that reflects that differences between the Cold War battlefield and more modern asymmetric warfare. SSGNs will be equipped with as many as 154 Tomahawk missiles.

Soviet Submarines

In submarines as in much else, the Soviets lagged behind their Western foes, and what they lacked in sophistication and accuracy they attempted to make up for in numbers. Their first subs were based on German models observed during World War II. By the late 1950s, they had deployed their first diesel and electric ballistic missile submarines, and in 1960 launched their first nuclear-powered subs. The Soviets, with their more limited budgets, were actually decades ahead of the Americans in one area: the SSGN, which they first began operating in the 1960s.

By 1980, the Soviet Union had 480 submarines, of which 71 were fast-attack craft and 94 SSBNs or SSGNs. Among these was the Alfa class, built in the 1970s, which

had 30-man crews and could achieve speeds of 43 knots (80 kph) and depths of 2,000 feet (600 m). The Typhoon class, first deployed in 1977, was the largest class of submarines ever built, at a length of 563 feet (172 m) and a beam of 81 feet (25 m). The Soviets, unlike the Americans, continued to build diesel-electric subs. Among these were the Kilo class, which first entered service in 1979 and are still being built for export.

Third World Submarines

From the early 1990s, it became apparent that the United States faced new challenges in the form of third-world nations armed with nuclear subs. Among these was Iran, which in 1993 deployed its first Kilo class subs in the Persian Gulf. Thus armed, the Teheran regime could close the Strait of Hormuz, through which one-quarter of the world's oil passes. Of the third-world countries that together possessed a total of 150 submarines, the largest share belonged to North Korea, with 25. Libya had six, as did Pakistan, whereas Pakistan's longtime foe India had 18.

Among the factors driving the sales to third-world countries was the collapse of the former Soviet Union, which had left Russia economically distressed and in need of hard currency. Given the fact that defense technology was one of the few areas in which the Soviet state had excelled, sales of submarines seemed a logical choice. Other, more prosperous Western European countries were also selling submarines to third-world countries, with Germany and France in the lead. At the same time, segments of the U.S. defense industry, facing downturns in production following the end of the Cold War, had begun to pressure Washington for an opportunity to gain a share of the emerging new markets in countries such as Egypt, Taiwan, and Argentina.

FURTHER READING:

PERIODICALS:

Ahrens, Frank. "Submarines, Examined at Depth: The Smithsonian's New Nautical Exhibit Settles in for a Three-Year Tour." *Washington Post.* (May 8, 2000): C1.

Arney, Kevin. "Midshipman Cruises Aboard Fast Attack Submarine." *The Officer* 73, no. 11 (November 1997): 57.

Lehman, John. "Silent, Deep, Deadly." *Wall Street Journal.* (November 11, 1998): 1.

Revelle, Daniel J., and Lora Lumpe. "Third World Submarines." *Scientific American.* (August 1994): 16–21.

ELECTRONIC:

Navy Fact File: Attack Submarines. U.S. Navy Office of Information. <http://www.chinfo.navy.mil/navpalib/factfile/ships/ship-ssn.html> (April 7, 2003).

Submarine Weapons. Smithsonian National Museum of American History. <http://americanhistory.si.edu/subs/weapons/index.html> (April 7, 2003).

SEE ALSO

Aircraft Carrier
Cruise Missile
P-3 Orion Anti-Submarine Maritime Reconnaissance Aircraft
USSTRATCOM (United States Strategic Command)

Unexploded Ordnance and Mines

MIKE LAMBERT

Munitions (devices equipped with explosives or other material for use in military operations) can represent a hazard to people and to any future use of the land where they are located. As either the accidental or deliberate remnants of military activity, they represent a growing humanitarian and environmental problem in many parts of the world. There are two general categories of these munitions. The first, unexploded ordnance (often abbreviated "UXO") can be defined as munitions that are left in place due to either not detonating as intended, or by deliberate abandonment once military operations have ceased. The second, mines, are a type of unexploded ordnance that are deliberately hidden and which are meant to cause damage to people or property at a later time.

Unexploded Ordnance

Unexploded ordnance is generally considered less dangerous than a mine because it is often found on the surface of the ground, although in many instances, unexploded ordnance can be feet or meters beneath the surface. Unexploded ordnance poses a potential hazard wherever it is found. Adults may attempt to collect unexploded ordnance as souvenirs or for resale as scrap metal. Children are at greater risk than adults because they are often attracted by the unusual objects and are unaware of the danger.

Types and occurrence of unexploded ordnance. The term ordnance refers to any munition, whether a bomb, bullet, grenade, or shell (or, strictly speaking, a mine) that contains an explosive device. Projectiles are ordnance that move and that can apply force through their own movement or inertia. The warhead of a projectile, containing the part of the munition intended to cause damage, can be a single unit or may be designed to fragment in operation. Bomblets are submunitions that are deployed separately from a parent munition, and a cluster bomb contains and disperses bomblets or submunitions. Cluster bombs were

In an effort to raise world attention about the dangers of unexploded land mines, Diana, Princess of Wales, watches a land-mine clearing demonstration in Huambo, central Angola, in 1997. AP/WIDE WORLD PHOTOS.

first deployed in the Vietnam War, and represent a growing source of danger from unexploded ordnance as they are used in more areas of combat.

When found on the sites of former ordnance supply depots, unexploded ordnance may be on the surface of the ground or just beneath the surface. At former bombing, artillery, or gunnery ranges, unexploded ordnance may be found at depths of several meters or feet if a projectile impacted the earth with considerable force and failed to detonate. The number of unexploded ordnance per acre depends on the size and intensity of use of a particular site. For example, the former Lowry Bombing Range in Colorado could have anywhere from 0.4 to 32 items of unexploded ordnance per acre, depending upon which organization is calculating the estimate (the smaller number comes from the U.S. Department of Defense, and the larger number is from the State of Colorado). On the other hand, the smaller but more intensively used former Southwest Proving Ground in Arkansas is estimated to contain 800 items of unexploded ordnance per acre.

Unexploded ordnance clearance program. The United States has made a systematic effort to clean up unexploded ordnance at former ordnance supply depots and military ranges. As recently as 1999, it was estimated that as many as 2,657 former military sites needed to be cleared of unexploded ordnance in the U.S., and by 2002, that number was raised to 9,000. The Defense Environmental Restoration Program (for) Formerly Used Defense Sites gives the U.S. Army Corps of Engineers the task of environmental restoration (including the cleanup of unexploded ordnance) at all former defense sites, regardless of which branch of the service was originally responsible for operating the site. The Corps follows a program of investigation and restoration that is specific to the needs of each site. This may include clearance of unexploded ordnance at the surface or to a specified depth. The actual detection of unexploded ordnance uses many of the same techniques used in mine clearance (discussed below). At the end of the restoration activity, the site may be approved for unrestricted future use, or may have its possible future uses restricted so as to limit exposure of people to the site. Also, long-term monitoring of the site may be instituted to insure that any unexploded ordnance missed by the restoration activity is not brought to the surface by erosion or the freeze-thaw cycle.

Mines

Mines, also called land mines, are a type of unexploded ordnance that will still function as originally intended. Usually carefully hidden in the shallow subsurface, they remain in place in order to explode in proximity to or in contact with a person or target. Because they can remain functional long after the end of the particular conflict in which they were deployed, mines create a lingering danger for anyone who comes near them. Originally developed for use in the American Civil War of the 1860s (where they were called torpedoes), mines from conflicts as long ago as World War I to as recent as the Balkan Wars of the 1990s are still causing injury today.

Mines come in a variety of designs, and new types of mines are constantly being developed to fill either an anti-personnel (death or injury of people) or anti-material (destruction or damage of equipment) function. They may be hidden individually, or in large numbers as a minefield so as to deny a potential adversary (or the local indigenous population) the use of a particular area. It has been estimated that as many as 60 people a day are killed by anti-personnel mines.

The United Nations has been involved in mine action (all aspects of mine education, detection, and removal) since it began working with the problem in Afghanistan in 1988. It acts primarily through the U.N. Department of Peacekeeping Operations, although eleven different departments or agencies within the U.N. are involved in some way with mine action. UNICEF (the United Nations Children's Fund) has been named the U. N. Focal Point for mine awareness education, and has published the U.N.'s International Guidelines for Landmine and Unexploded Ordnance Awareness Education. The International Committee of the Red Cross has its own mine/UXO awareness

programs that inform and work with affected communities that have mine problems. Humanitarian mine clearance is the removal of mines or unexploded ordnance under the auspices of a private humanitarian organizations (sometimes referred to as Non-Governmental Organizations, or NGOs), so as to allow the land to be used by the local community. One recent source lists 16 different such private organizations that are directly involved with mine and unexploded ordnance eradication, and eight other private organizations that work with communities affected by mines and unexploded ordnance.

Mine clearance (also called demining) has been described as consisting of two levels of activity. In the first level, which could be carried concurrently with a mine awareness program, an assessment is made of the scope of the problem through interviews and questionnaires given to the local population that is most directly affected by the presence of mines. The second level includes the location and removal of the mines. This may be done by a technique as simple as probing the ground with long sticks at regular intervals, exposing any solid objects that are encountered, and then removing any of the objects that turn out to be mines. Or, specially trained dogs may be employed to sniff out and indicate the location of explosives in the ground, followed by digging to reveal any mines and the subsequent removal of the mines.

Sophisticated electronic or geophysical methods have become widely used in the detection of both mines and other unexploded ordnance, and are utilized by demining technicians carrying detection equipment over the area to be examined for mines. These methods include electromagnetic induction (EMI), where an electrical current is induced and detected in buried metallic objects such as mine casings, and magnetometry that detects the distortions in the Earth's magnetic fields caused by buried ferrous objects. Conductive soils, interference from buried pipelines and artifacts, magnetic minerals, and plastic mine casings may cause difficulties in using these detection techniques. Ground penetrating radar (GPR) is not affected by these considerations, and instead reveals shapes of objects in the subsurface that might be mines. GPR is not considered to be as reliable as EMI or magnetometry, and the radar signal can be absorbed by vegetation or moisture in the soil. Newer technologies for use in mine detection include infrared (heat) imaging that detects the difference between how a buried mine and the surrounding soil retain or release heat. Vegetation interferes with this technique, and heat imaging can only detect mines within centimeters (inches) of the surface. Thermal neutron activation, already in use at some airports for detecting explosives in luggage, has also been proposed for the detection of explosives in buried mines. This would detect the high nitrogen content of explosives by bombarding the ground with neutrons and then looking for the specific gamma ray response of nitrogen. Problems with this technique include the need for a radioactive isotope as a source of gamma rays in the field.

In most cases, physical removal of mines in an area is still undertaken manually by technicians in the field, which is slow, labor-intensive, and dangerous. There are many mechanical systems for use in automated demining, such as large flail machines and milling machines, and proposed devices utilizing jets of water or lasers, but these have been criticized for their cumbersome nature and expense, the need for extensive logistical support, and the need to manually recheck areas where the machines have operated.

An international treaty to ban anti-personnel mines was signed by 122 nations in Ottawa, the capital of Canada, in December 1997. Formally entitled the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-personnel Mines and on Their Destruction, and less formally known as the Ottawa Convention, this treaty was ratified by 132 nations as of 2003. The United States is one of 62 nations that has not ratified the treaty.

FURTHER READING:

BOOKS:

Bryden, A., and A. McAslan. *Mine Action Equipment: Study of Global Operational Needs.* Geneva, Switzerland: Geneva International Centre for Humanitarian Demining, 2002.

Croll, M. *The History of Landmines.* Barnsley, South Yorkshire, Great Britain: Leo Cooper, 1998.

King, Colin, ed. *Jane's Mines and Mine Clearance.* Coulsdon, Surrey, Great Britain: Jane's Information Group, 1998.

McGrath, R. *Landmines and Unexploded Ordnance: A Resource Book* Sterling, Virginia: Pluto Press, 2000.

United States Environmental Protection Agency. *Interim Final Handbook on the Management of Ordnance and Explosives at Closed, Transferred, and Transferring Range.* Washington, D. C.: U.S. EPA Office of Solid Waste and Emergency Response, 2002.

PERIODICALS:

Loeb, V. "Unexploded Arms Require Big Cleanup at 16,000 U.S. Sites." *Washington Post.* November 25, 2002.

Sahlin, C., Jr. National Defense University Institute for National Strategic Studies, Washington, D.C. "Global Mine Clearance: An Achievable Goal?" *Strategic Forum* Number 43, 1998.

ELECTRONIC:

Lambert, M. "Unexploded Ordnance: a Reference Guide for the Citizen." Environmental Science and Technology Briefs for Citizens. 2001. <http://www.engg.ksu.edu/HSRC/Tosc/uxo.pdf> (April 25, 2003).

Canada Department of Foreign Affairs. "The Ottawa Convention Status Report." SAFELANE. April 2, 2003. <http://www.mines.gc.ca/convention-en.asp> (April 27, 2003).

UNICEF. "International Guidelines for Landmine and Unexploded Ordnance Awareness Education." United

Nations. 2002. <http://www.unicef.org/landguide/mineawar.pdf>(April 24, 2003).

United Kingdom, Counter-Terrorism Policy

TIMOTHY G. BORDEN

Prior to the September 11, 2001, terrorist attacks on the United States, counter-terrorism programs in the United Kingdom focused mainly on the Irish Republican Army (IRA), a militant group committed to ending British control of Northern Ireland. After the bombing of Pan Am Flight 103, on its way from London to New York, by Libyan terrorists in December 1988, the British government redoubled its domestic counter-terrorist efforts against a broader range of threats. Parliament also responded to the rise of fundamentalist religious terrorist groups by passing the Anti-Terrorism, Crime, and Security Act in 2001, an action that was criticized by many civil-rights groups.

Authorities in Northern Ireland detained suspected terrorists from the late 1950s onward during the IRA's "border campaign" of bombings. With a new wave of bombings under the IRA beginning in the late 1960s, including 153 bombings in 1970 alone, British authorities detained 2,000 suspected IRA members between 1971 and 1975. After bombs exploded in two pubs in Birmingham, England in November 1974, killing 21 and injuring 162 others, Parliament passed the Prevention of Terrorism (Temporary Provisions) Act of 1974. The act allowed authorities to arrest suspected terrorists without a warrant and detain them for up to a week without filing charges against them. Suspected terrorists could also be deported from England to Northern Ireland.

The policy of internment raised international criticism, as did the practice of "hooding," in which detainees would be isolated and forced to wear hoods over their heads. After an investigation by the European Commission of Human Rights in 1976, the practices of food and sleep deprivation, noise bombardment, forced standing at attention, and hooding were condemned by the body. Despite the commission's decision, the practices continued. Some historians assert that the counter-terrorist policies contributed to an increase of IRA violence in retribution, as 2,161 people died in the 1970s in the conflict between the IRA and British authorities.

Whereas the counter-terrorist campaign against the IRA relied on military force, surveillance, and other covert and overt measures, there was a notable emphasis on technology in the wake of the Pan Am Flight 103 bombing in 1988. Libyan terrorists had successfully hidden plastic explosives on the flight, which sent the aircraft plummeting into the village of Lockerbie, Scotland, after they detonated. In response, the British Airports Authority (BAA) undertook an extensive reevaluation of its security measures. The BAA reforms resulted in a five-stage system to screen all checked baggage at British airports, including x-ray machines and later, three-dimensional scanners and equipment that could detect trace elements of explosive devices. All passengers at BAA airports were also screened through x-ray machines and metal detectors and a predetermined number of passengers were individually hand searched by security officers. All carryon items were also x-rayed and articles that failed to pass inspection were individually inspected. Although the measures were sufficient to prevent terrorists from attacking a BAA facility or the planes that ran through them, a series of robberies in 2002 on BAA runways demonstrated that the system still had flaws.

In December 2001, British Parliament passed the Anti-Terrorism, Crime, and Security Act. The law allowed authorities to detain suspected terrorists for up to six months without filing charges and for additional six-month periods after reviewing the suspect's case. It also retained provisions that made it a crime to fail to report information on terrorist activities. In order to allay fears of civil-rights advocates, a provision was added to limit the powers of police and other security services from looking through confidential records.

FURTHER READING:

BOOKS:

English, Richard. *Armed Struggle: A History of the IRA.* New York: Oxford University Press, 2003.

Geraghty, Tony. *The Irish War: The Hidden Conflict between the IRA and British Intelligence.* Baltimore: Johns Hopkins University Press, 2000.

Gerson, Allan. *The Price of Terror: Lessons of Lockerbie for a World on the Brink.* New York: HarperCollins, 2001.

Taillon, J. Paul de B. *The Evolution of Special Forces in Counter-terrorism: The British and American Experiences.* Westport, Conn.: Greenwood Publishing Group, 2000.

ELECTRONIC:

British Airports Authority. "About BAA." <http://www.baa.co.uk/main/corporate/about_baa/our_business/security_page.html> (March 5, 2003).

Human Rights Watch. "U.K.: New Anti-Terror Law Rolls Back Rights." <http://www.hrw.org/press/2001/12/UKbill1214.htm> (March 5, 2003).

SEE ALSO

Airline Security
Bomb Detection Devices
Intelligence and Democracy: Issues and Conflicts
Interrogation: Torture Techniques and Technologies
MI5 (British Security Service)
MI6 (British Secret Intelligence Service)

Pan Am 103 (Trial of Libyan Intelligence Agents
Interrogation: Torture Techniques and Technologies

United Kingdom, Intelligence and Security

The intelligence community of the United Kingdom is both older and more complicated than that of the United States. MI5, or the Security Service, and MI6, the Secret Intelligence Service, are the best-known components of the British intelligence structure, but these are just two parts of a vast intelligence apparatus. Command and control operates through no less than four entities: the Central Intelligence Machinery, the Ministerial Committee on the Intelligence Services, the Permanent Secretaries' Committee on the Intelligence Services, and the Joint Intelligence Committee. Communications intelligence is the responsibility of the Government Communications Headquarters (GCHQ), which works closely with the Communications Electronics Security Group, while a number of agencies manage military intelligence under the aegis of the Ministry of Defense. Even London's Metropolitan Police, or Scotland Yard, has its own Special Branch concerned with intelligence.

The principal oversight committee for British intelligence is the Central Intelligence Machinery, based in the Prime Minister's Cabinet Office. Roughly analogous, in various ways, to the U.S. National Security Council, Intelligence Community, and intelligence committees in both houses of Congress, it oversees the coordination of security and intelligence agencies. The Central Intelligence Machinery acts as a mechanism for assessment and accountability, observing and reporting on the performance of specific agencies. It is also concerned with tasking and the allocation of resources.

Whereas the Central Intelligence Machinery is at the top echelon of command and control, the Ministerial Committee on the Intelligence Services exercises regular ongoing oversight of intelligence activities. Through this committee, the Prime Minister, with the assistance of the Secretary of the Cabinet, exercises authority over the daily operations of the British intelligence and security communities as a whole. The Home Secretary oversees MI5, the National Criminal Intelligence Service, and Scotland Yard, while MI6 and GCHQ answer to the Foreign and Commonwealth Secretary.

These ministers receive assistance from the Permanent Secretaries' Committee on the Intelligence Services. Finally, the Joint Intelligence Committee, or JIC, is not unlike America's National Intelligence Council, which prepares National Intelligence Estimates. JIC draws up general intelligence needs to be met by GCHQ and MI6.

MI5 and domestic security. The "MI" by which the two principal British security services are known (MI5, or Security Service, and MI6, or Secret Intelligence Service) refers to their common origins in military intelligence. Both can trace their roots to the Secret Service Bureau, created in 1909 after a report by Parliament's Committee on Imperial Defense concluded that "an extensive system of German espionage exists in this country. . ." Working with the War Office, Admiralty, and various operatives and agents overseas, the bureau had both a Home Section and a Foreign Section—precursors, respectively, of MI5 and MI6.

After the outbreak of World War I, the War Office took over the Home Section, designated MI5 in 1916. MI5, which might be likened to the U.S. Federal Bureau of Investigation (although its operatives do not have arrest powers), spent the war years successfully apprehending a number of German spies and saboteurs in England, and after the war directed its attention against Communist elements. By the late 1930s, MI5's focus once again became German and pro-German infiltrators, of which it captured several. During the Cold War, MI5 returned to the efforts against Communists that had concerned it in the interwar years, but was less successful in this, due to the discovery of numerous Soviet moles within its ranks. Today, MI5 is concerned with counter-terrorism and counter-espionage against groups in Northern Ireland, as well as terrorist organizations based in the Middle East and other parts of the world.

Scotland Yard. The Metropolitan Police is better known by a name that refers to the location of its original headquarters, which overlooked a residence formerly owned by Scottish royalty. Scotland Yard, established in 1829, has a number of intelligence and surveillance units. Among these is the Scientific Intelligence Unit, which is concerned with behavioral and DNA analysis relating to unsolved crimes. The unit scored a major victory in 1986, when it became the first police organization in the world to track down a rapist and murderer—the perhaps appropriately named Colin Pitchfork—by use of DNA evidence.

Scotland Yard formed the world's first antiterrorism unit in 1883, when it established the Special Irish Branch in response to bombings in London committed by the Irish Fenian movement. The office later became known as the Special Branch. Providing protective services for Queen Victoria and later monarchs, the Special Branch performed a function akin to that of the U.S. Secret Service. The Special Branch also assists MI5 with a number of activities that include surveillance, arrest (a power that Special Branch officers possess), and testimony at trial. This last duty helps preserve the cover of MI5 officers, who are rarely allowed to testify in public to minimize risk of exposure.

National Criminal Intelligence Service. In addition to its other responsibilities, Scotland Yard operates the National Identification Service, which includes the National Criminal

Record Office and National Fingerprint Collection. Despite these efforts at gathering criminal intelligence, in the 1980s the Home Secretary's office recognized the need for better coordination of these intelligence-gathering efforts, and in April 1992, established the National Criminal Intelligence Service (NCIS).

Directed toward criminal organizations operating within the country, NCIS is one of Europe's first national criminal intelligence services. Its staff of some 500 personnel has backgrounds in police, customs, and excise work. Its areas of interest range from organized crime, drug trafficking, and money laundering to child molestation and football hooliganism.

MI6 and international intelligence. MI6 (formerly the Secret Service Bureau Foreign Section) gained its present designation in 1921. From it would emerge the precursor to GCHQ in 1919. Analogous to the U.S. Central Intelligence Agency (CIA), MI6 directed its efforts toward more or less the same threats targeted by MI5: Germans during the world wars, and Communists during the interwar and postwar periods. In World War II, MI6 sponsored aerial reconnaissance efforts that would later be taken over by the Royal Air Force (RAF).

Through GCHQ, MI6 enjoyed a number of successes during World War II, most notable among them being the Ultra program to break German Enigma ciphers. Like MI5, however, MI6 in the early Cold War experienced embarrassment with the exposure of Soviet spy rings operating in its midst. Yet MI6 also scored a victory by cultivating a Soviet mole in Oleg Penkovsky, who went on to work with both MI6 and CIA. Whereas MI5 established an atmosphere of openness in the post-Cold War era, MI6, which continues to operate extensively abroad, remains highly secretive.

GCHQ. GCHQ grew out of the Government Code and Cypher School (GC&CS), established in November 1919. During the 1920s and 1930s, GC&CS had considerable success in its efforts to decipher German and Soviet transmissions. Once the Germans acquired the Enigma machine, with its apparently unbreakable ciphers, in the late 1930s, GC&CS greatly stepped up its efforts. In August 1939, just before war broke out in Europe, it moved its headquarters to Bletchley Park outside London. There its cryptanalysts undertook Operation Ultra, the breaking of the Enigma cipher—a project whose details remained classified until the 1970s.

Renamed the Government Communications Headquarters in 1942 to conceal its activities, this leading communications intelligence agency of the United Kingdom—quite similar in function to the U.S. National Security Agency (NSA)—greatly escalated its efforts in the Cold War. GCHQ is also like NSA, with which it participates in the Echelon global surveillance network, in its level of secrecy. Much of what is known about it comes from James Bamford's famous 1982 book on NSA, *The Puzzle Palace.*

According to Bamford, GCHQ at that time had six directorates. Among these were the Composite Signals Organization, dedicated to radio intercepts; the Directorate of Organization and Establishment, whose functions were chiefly administrative; the Directorate of Signals Intelligence Plans, concerned with long-range planning and management; and the Joint Technical Language Service, which intercepted foreign communications. The Directorate of Signals Intelligence Operations and Requirements, which was the largest and most secretive of directorates, according to Bamford, oversaw codebreaking activities.

Bamford also named the Directorate of Communications Security, whose activities were affiliated with an agency about which somewhat more is known, the Communications Electronics Security Group, or CESG. Established in 1969, CESG is the British national technical authority for information security, and works with a number of government agencies to ensure that communications security is maintained through state-of-the-art equipment. At the end of the Cold War, GCHQ employed some 6,000 people, but its staff had decreased to about 4,500 by the mid-1990s.

Military intelligence. In addition to the Cabinet-level oversight committees mentioned earlier, the Minister of Defense controls military intelligence through the Defence Procurement Executive and the Defense Intelligence Staff (DIS). DIS in turn oversees a number of military intelligence agencies, most notably the Defense Geographic and Imagery Intelligence Agency (DGIA) and the Defense Intelligence and Security Center.

DGIA was formed in 2000 from the merger of the RAF's Joint Air Reconnaissance Intelligence Center (JARIC) and the Military Survey Defense Agency. JARIC was concerned with aerial reconnaissance and the capture of photographic intelligence, and the Military Survey with geographic and geospatial support to defense planning. The Defense Intelligence and Security Center, created in 1996, integrates intelligence and security training for Britain's military services.

■ FURTHER READING:

BOOKS:

Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence.* Woodstock, NY: Overlook Press, 2002.

Andrew, Christopher M. *Her Majesty's Secret Service: The Making of the British Intelligence Community.* New York: Viking, 1986.

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency.* Boston: Houghton Mifflin, 1982.

Bar-Joseph, Uri. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain.* University Park: Pennsylvania State University Press, 1995.

Dorril, Stephen. *MI6: Inside the Cover World of Her Majesty's Secret Intelligence Service.* New York: Free Press, 2000.

Pincher, Chapman. *The Spycatcher Affair.* New York: St. Martin's Press, 1988.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1998.

West, Nigel. *Molehunt: Searching for Soviet Spies in MI5.* New York: W. Morrow, 1989.

Winterbotham, F. W. *The Ultra Secret.* New York: Harper & Row, 1974.

Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer.* New York: Viking, 1987.

ELECTRONIC:

Communications Electronics Security Group. <http://www.cesg.gov.uk/> (April 12, 2003).

Government Communications Headquarters. <http://www.gchq.gov.uk/> (April 12, 2003).

The Metropolitan Police Service. <http://www.met.police.uk/> (April 12, 2003).

MI5: The Security Service. <http://www.mi5.gov.uk/> (April 11, 2003).

United Kingdom Intelligence Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/uk/index.html> (April 11, 2003).

SEE ALSO

Bletchley Park
British Terrorism Act
Echelon
MI5 (British Security Service)
MI6 (British Secret Intelligence Service)
Official Secrets Act, United Kingdom
Special Relationship: Technology Sharing Between the Intelligence Agencies of the United States and United Kingdom
Ultra, Operation
United Kingdom, Counter-terrorism Policy
United States, Intelligence and Security

United Nations Security Council

ADRIENNE WILMOTH LERNER

The United Nations Charter was ratified by its founding members on October 24, 1945. Three years later, the member nations convened the first official meeting of the Security Council, as well as the other UN committees. The outstanding mission of the entire United Nations organization is to promote global peace and good relations among nations. The Security Council fulfills the UN mission through diplomacy, sanctions, and peacekeeping operations.

Membership, organization, and voting. The United Nations is divided into one large meeting body, the General Assembly, and three smaller operational committees. Every member nation, as well as observer missions, is represented in the General Assembly, and on two committees, the Economic and Social Council and the Trusteeship Council. Membership in the third and most powerful UN committee, the Security Council, is selected by established protocol. Five nations, reflecting the global balance of power when the United Nations was created, have permanent membership on the Security Council: the United States, Britain, France, Russia, and China. The ten other seats on the Security Council are filled by UN member states on a rotating basis, for two terms. The presidency of the Security Council changes every month, rotating according to the English alphabetical listing of represented countries.

The Security Council itself is divided into two standing committees, the Committee of Experts on Rules of Procedure and the Committee on the Admission of New Members. The council contains several *ad hoc* committees, which are created to draft resolutions, investigate issues, and mediate conflicts. Working groups are often formed to conduct preliminary, investigative research on a resolution, or to facilitate the evolution of policy regarding a long-standing crisis.

In the UN General Assembly, each member state has one vote. The same applies to voting on resolutions within the Security Council. Passage of a resolution requires either a simple majority or a two-thirds majority, depending on the rule of parliamentary procedure under which the vote was called. However, the permanent members of the Security Council reserve special voting rights. Permanent members reserve the right of veto, or the ability to strike down resolutions with their singular vote.

Under the rules of the UN charter, the Security Council must meet at least once every year. However, the Security Council is designed to operate continuously. The non-permanent seats have staggered terms, so that the council changes five members every year, instead of ten members every two years. One member of each national delegation to the Security Council must be present at the United Nations at all times so the council can meet on a moments notice. On the few occasions that the council has met at a location other than the United Nations, Security Council member states observed this rule by leaving a member of their delegation at headquarters.

Duties of the Security Council. The Security Council's main objective is the promotion of peace. To that end, the council has at its disposal several means of dispute resolution, ranging from mediation to military action. When a threat against international peace is brought to the attention of the Security Council, the council first attempts to

The United Nations Security Council stands to observe a moment of silence during their meeting on September 12, 2001. The council approved a draft resolution condemning the terrorist attack on New York's World Trade Center. ©AFP/CORBIS.

negotiate a settlement between the disputing parties. The council may use its own member delegations, refer the issue to discussion in the General Assembly, or appoint the Secretary-General, the head of the United Nations, to act as mediator.

If no peaceful agreement can be reached, and the disputing factions use violence, intimidation, or force, the Security Council can then enact policy resolutions to solve the conflict or restore peace. Sometimes this policy includes economic sanctions, such as trade embargoes or prohibitions on governments borrowing from international funds. Under the Security Council regulations, however, humanitarian aid can never be withheld from any nation or group of people. In the past, the United Nations has applied sanctions to nations in violation of non-proliferation of weapons agreements, or whose governments perpetuated human rights crimes. The Security Council also reserves the right to recommend expulsion of any UN member state in gross violation of the UN charter and international law, though the dismissal must be voted on and passed in the General Assembly.

The Security Council is the only United Nations organization that can authorize military action and maintain a military-trained peacekeeping force. In violent international dispute, the Security Council can send intervening peacekeeping troops to secure areas in turmoil. Peacekeeping forces are supplied by various individual UN member states but under the direction of UN command. Peacekeeping forces do not participate in the military agenda of any specific member state, and are neutral in all disputes. The role of peacekeeping troops in the international community is to preserve order, to protect civilian infrastructure and safety, and guard the delivery of humanitarian aid to better facilitate the diplomatic resolution of conflicts.

The Security Council is further responsible for overseeing compliance with international agreements involving weapons, the rules of engagement (conduct during war), the illegal spread of nuclear technology, and other threats to international peace. To enforce these treaties, such as international agreements on nuclear non-proliferation, the Security Council can authorize UN-led inspections of a nation's military arsenal. In addition, the Security Council can order sanctions or authorize military action.

Impact on the international community. Actions taken by the United Nations Security Council have had a significant impact on the international community, with varying success. Long-standing sanctions against South Africa helped end the nation's practice of apartheid and rehabilitated its standing in the international community. On the other

hand, resolutions and UN mandates regarding the Palestinian-Israeli conflict have been frequently breached, and those enforced failed to abate violence in the region. In the past decade, the Security Council has intervened in conflicts in from Bosnia to western Africa. Though peacekeepers in most tumultuous regions have managed to help dissemination of humanitarian aid and enforce the rule of law, root diplomatic solutions have lagged behind.

In 2002 and 2003, the UN Security Council was at loggerheads over the question of Iraq. Although the entire Assembly voted in favor of weapons inspections in the nation, the issue of subsequent military intervention was contentious. The United States and Great Britain, as well as other UN member nations, opted to invade Iraq to overthrow the regime of Saddam Hussein without the express consent of a new, specific Security Council resolution, but with the implied consent of previous Resolution 1441. However, United Nations organizations have continued to provide humanitarian aid to the region.

In early 2003, the Security Council supervised fifteen ongoing peacekeeping missions and considered resolutions seeking to implement more. In its almost sixty-year tenure, the Security Council has authorized 55 separate peacekeeping operations. Holding to the principles of the UN charter, many nations participate in ongoing peacekeeping efforts.

FURTHER READING:

ELECTRONIC:

United Nations. <http://www.un.org> (1 April 2003).

OTHER:

United Nations. *Sources: Basic Facts about the United Nations.*Sales No.E.98.I.20., Press Release GA/9784, 2000.

SEE ALSO

Bosnia, Intelligence and Security
IMF (International Monetary Fund)
Nonproliferation and National Security, United States
Weapons of Mass Destruction, Detection
World War II

United Self-Defense Forces/ Group of Colombia (AUC *Autodefensas Unidas de Colombia*)

The United Self-Defense Forces/Group of Colombia (AUC *Autodefensas Unidas de Colombia*)—commonly referred to as the paramilitaries—is an umbrella organization formed in April 1997 to consolidate local and regional paramilitary groups each with the mission to protect economic interests and combat insurgents locally. AUC is supported by economic elites, drug traffickers, and local communities lacking effective government security. AUC claims its primary objective is to protect its sponsors from insurgents. The AUC now asserts itself as a regional and national counterinsurgent force. It is adequately equipped and armed and reportedly pays its members a monthly salary. AUC political leader Carlos Castaño has claimed 70% of AUC's operational costs are financed with drug-related earnings, the rest from "donations" from its sponsors.

Organization activities. AUC operations vary from assassinating suspected insurgent supporters to engaging guerrilla combat units. Colombian National Combat operations generally consist of raids and ambushes directed against suspected insurgents. The AUC generally avoids engagements with government security forces and actions against U.S. personnel or interests.

The AUC is estimated to have 6000 to 8150 members, including former military and insurgent personnel. AUC forces are strongest in the northwest in Antioquia, Córdoba, Sucre, and Bolívar Departments. Since 1999, the group demonstrated a growing presence in other northern and southwestern departments. Clashes between the AUC and the Revolutionary Armed Forces of Colombia (FARC) insurgents in Putumayo in 2000 demonstrated the range of the AUC to contest insurgents throughout Colombia.

FURTHER READING:

ELECTRONIC:

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Taylor, Francis X. U.S. Department of State. Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing. May 21, 2002 <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17,2003).

U.S. Department of State. Annual Reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

SEE ALSO

Terrorism, Philosophical and Ideological Origins
Terrorist and Para-State Organizations
Terrorist Organization List, United States
Terrorist Organizations, Freezing of Assets

United States, Counter-Terrorism Policy

JUDSON KNIGHT

The foundation of the United States counterterrorism policy, according to the U.S. State Department Coordinator for Counterterrorism, are embodied in four principles:

The National Center for the Study of Counter-Terrorism and Cyber-Crime on the campus of Norwich University in Northfield, Vermont, when fully operational, will focus on security concerns from miniaturizing communications devices to combatting attacks on computer networks. AP/WIDE WORLD PHOTOS.

the government makes no concessions to or agreements with terrorists; terrorists must be brought to justice for their crimes; states that sponsor terrorists and terrorism must be isolated and pressured so as to force a change of behavior; and the counterterrorism capabilities of countries allied with the United States, and those that require assistance in fighting terrorism, must be bolstered. President William J. Clinton outlined U.S. policy on terrorism in Presidential Decision Directive (PDD) 39 in 1995, and in 1998 he made specific provisions for combatting terrorism in PDD 62. Since the terrorist attacks of September 11, 2001, the face of U.S. counterterrorism has changed considerably, with the signing of the Patriot Act as well as a number of other measures. Among these is a refocusing of the nation's leading law enforcement organization, the Federal Bureau of Investigation (FBI), toward a mission increasingly concerned with counterterrorism.

Deterrence and the Reduction of Vulnerabilities

These four principles provide a framework for U.S. policy. For example, when President George W. Bush sent U.S. troops into combat in Afghanistan in October 2001, and in Iraq in March 2003, this action was in line with the third principle, pressuring nations that support terrorism. Yet, even before September 2001, these principles were in place, and have guided the policy of successive administrations, whether controlled by Republicans or Democrats.

Issued by Clinton on June 21, 1995, just two months after the Oklahoma City bombing, PDD 39 was titled "U.S. Policy on Counterterrorism." Its purpose was to provide guidelines for deterring terrorism on America's shores, as well as terrorism against Americans and allies abroad.

PDD 39 ordered the Attorney General, the Director of the FBI, the Director of Central Intelligence (DCI), and the secretaries of State, Defense, Transportation, and Treasury, to enact measures to reduce vulnerabilities to terrorism. Also critical in this regard are the General Accounting Office (GAO), whose responsibilities include national preparedness, and the General Services Administration (GSA), which, as overseer of government building projects, has been increasingly tasked toward providing structural protections against attacks such as those at Oklahoma City or the World Trade Center.

The directive, only part of which has been declassified, also addressed deterrence of terrorism. It called for the return of indicted terrorists to the United States for prosecution, and presented measures (classified as of 2003) for dealing with states that support terrorism. In PDD 62, issued on May 22, 1998, Clinton established the National Coordinator for Security, Infrastructure Protection and Counterterrorism, while PDD 63 created the Critical Infrastructure Assurance Office (CIAO).

Although the functions of CIAO and the national coordinator were similar, they reported along quite different chains of command. Whereas CIAO, now part of the Department of Homeland Security (DHS), was then part of the Department of Commerce, the national coordinator reported to the National Security Council (NSC). Given the fact that the NSC is the president's advisory board on national security affairs, this fact signaled the importance of the new national coordinator.

The Patriot Act. The leading statement of deterrence policy since September 2001, is the Patriot Act, which Bush signed into law on October 26, just six weeks after the attacks. The law contained changes to some 15 different statutes, and its provisions collectively gave the Justice Department and its agencies a number of new powers in intelligence-gathering and criminal procedure against drug trafficking, immigration violations, organized criminal activity, money laundering, and terrorism and terrorism-related acts themselves.

Among its specific provisions, the Patriot Act gave increased authority to intercept communications related to an expanded list of terrorism-related crimes; allowed investigators to aggressively pursue terrorists on the Internet; provided new subpoena power to obtain financial information; reduced bureaucracy by allowing investigators to use a single court order for tracing a communication nationwide; and encouraged sharing of information between local law enforcement and the Intelligence Community.

The Patriot Act also provided for the creation of a "terrorist exclusion list" (TEL). Members of organizations listed on the TEL may be prevented from entering the country, and in certain circumstances may be deported. Before the Secretary of State places an organization on the TEL, he or she must find that its members commit or incite terrorist activity, gather information on potential targets for terrorist activity, or provide material support to further terrorist activity.

Assignments for Specific Agencies

In its provisions for responding to terrorism, PDD 39 designated the State Department as the lead agency for attacks on civilians outside of the United States. It also established the State Department Foreign Emergency Support Team (FEST) and the FBI's Domestic Emergency Support Team (DEST).

The directive gave the Federal Aviation Administration (FAA) authority to deal with "air piracy," and assigned authority over hijackings to the Department of Justice, working in concert with the departments of State, Defense, and Transportation. That particular part of PDD 39 has been superseded by the Aviation and Transportation Security Act (ATSA). Signed into law by President Bush on November 19, 2001, the ATSA created the Transportation Security Administration (TSA), now part of the Department of Homeland Security (DHS).

In its consequence management provisions, PDD 39 gave the Federal Emergency Management Agency (FEMA) the responsibility of developing an overall federal response plan, and ensuring that states developed their own plans. This provision of PDD 39 is just one of many statements of policy on the coordination of consequence management responsibilities, which involve an array of departments, agencies, and offices, most notably FEMA, the Environmental Protection Agency (EPA), and the Coast Guard.

Nearly a decade earlier, for instance, Congress in 1986 passed the Emergency Planning and Community Right-to-Know Act (EPCRA), which established guidelines for assistance of local communities by federal agencies in the event of a toxic chemical spill or related incident. EPCRA also provides a framework for action both by citizens and state governments. Since the time of its passage, EPCRA and similar provisions have been increasingly understood to deal also with terrorist incidents, which may involve unleashing of lethal substances.

Similarly, in 1985, a FEMA committee had drawn up the Federal Radiological Emergency Response Plan (FRERP), a blueprint for the response of the U.S. federal government to a radiological emergency—that is, a crisis involving the release of nuclear radiation. The FRERP is an agreement among 17 federal agencies, key among which are FEMA, the Nuclear Regulatory Commission (NRC), the Departments of Energy and Defense, and the EPA.

Also important is the Coast Guard, which, in addition to protecting ports and shorelines, operates the National Response Center. The latter is the sole national point of contact for reports of oil spills, as well information regarding discharges of chemical, radiological, and biological discharges into the environment.

Agencies tasked for counterterrorism. Myriad government intelligence, security, and law enforcement agencies have a counterterrorism function. Most obvious among these are various components of the U.S. military, most notably Delta Force and Seal Team Six. These special teams, along with the larger Special Operations Command, are the "muscle" of U.S. counterterrorism. Highly trained and well-equipped with state-of-the-art weaponry, airborne insertion equipment, and other forms of technology, elite counterterrorist teams are capable of rescuing hostages and eliminating terrorists in situations for which regular military forces would be inappropriate.

Equally vital is the work of the Coordinator for Counterterrorism. In accordance with the fourth major principle of U.S. counterterrorism policy, the coordinator is charged by the Secretary of State with coordinating efforts to improve cooperation between the U.S. government and its foreign counterparts in battling terrorism. An ambassador, the coordinator is the primary functionary of the

federal government for developing and implementing America's counterterrorism policy.

DCI Counterterrorist Center. In an entirely different wing of government is the DCI Counterterrorist Center (CTC). Though part of the CIA, the CTC is under more direct control by the DCI than are most CIA activities, a sign of the significance attached to counterterrorism. During the mid-1980s, a panel led by then–Vice President George Bush studied U.S. efforts against terrorism and concluded that, while U.S. agencies collected information on foreign terrorism, they did not aggressively operate to disrupt terrorist activities. On these recommendations from Bush, himself a former DCI, William Casey established the CTC.

The mission of the CTC is to assist the DCI in coordinating the counterterrorism efforts of the Intelligence Community by implementing a comprehensive counterterrorist operations program, and by exploiting all sources of intelligence to produce in-depth analyses of terror groups and their state supporters. CTC collects information on these groups, and when it has credible information of a threat, issues warnings. Alongside it is the Interagency Intelligence Committee on Terrorism, an Intelligence Community board that assists the DCI in coordinating intelligence-gathering efforts against terrorists. In the 1990s, the CTC began working closely with the FBI, and in 1996 they exchanged senior-level officers to manage the counterterrorist offices of both agencies.

The FBI. Prior to September 2001, the mission of the FBI had been strictly that of a law-enforcement agency, but in the wake of September 11, Attorney General John Ashcroft and FBI Director Robert S. Mueller III refocused the bureau's efforts toward counterterrorism. In December 2001, Mueller announced plans to reorganize headquarters by creating new counterterrorism, cybercrimes, and counterintelligence divisions, by modernizing information systems, and emphasizing relationships with local first responders.

By the Spring of 2002, criticism of Mueller's plans was on the rise, with detractors maintaining that the measures were not thorough enough. To this end, Mueller announced a number of new reforms. These included the hiring of 400 more analysts, including 25 from the CIA; the retasking of 480 special agents from white-collar and violent crimes to counterterrorism; the creation of an intelligence office; development of terrorism expert support teams to work with the bureau's 56 field offices; recruitment of Arabic speakers and others fluent in Middle Eastern and South Asian languages; creation of a joint terrorism task force to coordinate with the CIA and other federal agencies; and the improvement of financial analysis and other forms of strategic analysis directed toward terrorist groups.

In January 2003, President Bush announced plans to create a new counterterrorism intelligence center that would bring together intelligence collected domestically with that gathered overseas. This idea had been in development for some time, but one major issue of dispute was the question of which agency, the FBI or CIA, should manage the new center. One proposal put forward at the time involved the expansion of the DCI Counterterrorist Center, the oldest office of its kind. In February, Bush unveiled the organizational blueprint for the new unit, which would bring together FBI and CIA efforts under the aegis of a Terrorist Threat Integration Center, headed by the CIA.

■ FURTHER READING:

BOOKS:

Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign against Terrorism.* Washington, D.C.: CSIS Press, 2001.

Chapman, Robert, et. al. *COPS Innovations: A Closer Look: Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness.* Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2002.

Combatting Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism. Washington, D.C.: General Accounting Office, 2000.

PERIODICALS:

Deutch, John. "Smarter Intelligence." *Foreign Policy* no. 128 (January/February 2002): 64–69.

Eggen, Dan, and Jim McGee. "FBI Rushes to Remake Its Mission: Counterterrorism Focus Replaces Crime Solving." *Washington Post.* (November 12, 2001): A1.

Eggen, Dan. "Bush Aims to Blend Counterterrorism Efforts." *Washington Post.* (February 15, 2003): A16.

Haque, M. Shamsul. "Government Responses to Terrorism: Critical Views of Their Impacts on People and Public Administration." *Public Administration Review* 62 (September 2002): 170–80.

Pincus, Walter, and Mike Allen. "Terrorism Agency Planned: Center to Integrate Intelligence, Analysis." *Washington Post.* (January 29, 2003): A12.

ELECTRONIC:

Coordinator for Counterterrorism. United States Department of State. <http://www.state.gov/s/ct/> (February 22, 2003).

Counterterrorism Policy. University of Pittsburgh School of Law. <http://jurist.law.pitt.edu/terrorism/terrorism2.htm> (May 1, 2003).

Terrorism/Counter-Terrorism Web Links. United States Institute of Peace. <http://www.usip.org/library/topics/terrorism.html> (May 1, 2003).

SEE ALSO

Canada, Counter-terrorism Policy
Chemical and Biological Defense Information Analysis Center (CBIAC)
Chemical safety: Emergency Responses
Coast Guard National Response Center

Coordinator for Counterterrorism, United States Office
DEA (Drug Enforcement Administration)
Delta Force
Domestic Emergency Support Team, United States
Domestic Intelligence
Domestic Preparedness Office (NDPO), United States National
Emergency Response Teams
France, Counter-terrorism Policy
FEST (United States Foreign Emergency Support Team)
EPA (Environmental Protection Agency)
FEMA (United States Federal Emergency Management Agency)
GAO (General Accounting Office, United States)
General Services Administration, United States
Germany, Counter-terrorism Policy
Infrastructure Protection Center (NIPC), United States National
Israel, Counter-terrorism Policy
Law Enforcement, Responses to Terrorism
National Preparedness Strategy, United States
National Response Team, United States
NNSA (United States National Nuclear Security Administration)
Nuclear Emergency Support Team, United States
Nuclear Regulatory Commission (NRC), United States
SEAL Teams
Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator
United Kingdom, Counter-terrorism Policy

United States, Intelligence and Security

JUDSON KNIGHT

The United States intelligence and security apparatus is a vast collection of departments, agencies, and offices. It is not a single monolithic entity, although within it is a unified, decentralized group of 14 intelligence and security organizations known as the Intelligence Community (IC). The Intelligence Community is overseen by the director of the Central Intelligence Agency (CIA), the most well known of intelligence organizations in the United States, and includes the nation's most prominent law-enforcement organization, the Federal Bureau of Investigation (FBI), as well as many others. In addition to the Department of Defense (DOD), entities involved in national security include the departments of Justice, the Treasury, Homeland Security (DHS), Energy, Commerce, and Transportation. In terms of national security as a whole, departments such as Agriculture, Health and Human Services, and the Interior also have a role to play, as do independent agencies, including the Federal Emergency Management Agency (FEMA), the Environmental Protection Agency (EPA), General Services Administration (GSA), and General Accounting Office (GAO).

Oversight of the IC in particular, and intelligence and security activities in general, comes from both the executive and legislative branches of government. The President, acting partly through the National Security Council (NSC), oversees intelligence and acts as commander-in-chief of the armed forces, a key component of security. Additionally, both houses of Congress exert influence through intelligence committees, and through their ultimate control over intelligence and security budgets.

The power of Congress over intelligence and security is exerted at a greater remove than that of the president, whose Executive Office oversees the NSC and other functions. The NSC consists of the president, the vice president, and the secretaries of State and Defense. Leadership comes from the president, often acting with, or through, the Assistant to the President for National Security Affairs—a role better known by the informal title National Security Advisor. The NSC can and usually does involve other Cabinet-level departments with a stake in national security.

In addition to the NSC, offices at the White House associated with intelligence and security include the Senior Director for Intelligence Programs; the National Coordinator for Security, Infrastructure Protection, and Counterterrorism; and the Office of National Drug Control Policy.

Particularly critical is the President's Foreign Intelligence Advisory Board (PFIAB), which reviews the activities and performance of all agencies involved in intelligence and advises the president on its assessments. Under the aegis of the PFIAB is the three-member Intelligence Oversight Board, responsible for reviewing the legality and propriety of intelligence activities.

Among agencies that operate at a national level are the Chemical and Biological Defense Information Analysis Center, Interagency Operational Security Support Staff, National Interagency Counterdrug Institute/National Interagency Civil-Military Institute, the Security Policy Board, and the Technical Support Working Group.

The Intelligence Community

Central to U.S. intelligence and security are the 14 members of the Intelligence Community (IC). In addition to the CIA, the IC includes 13 other agencies and organizations, of which most are part of DOD. DOD members of the IC include the Defense Intelligence Agency (DIA), National Security Agency (NSA), National Reconnaissance Office (NRO), National Imagery and Mapping Agency (NIMA), and the intelligence agencies of the Army, Navy, Air Force, and Marine Corps. Non-DOD members include the FBI (a part of the Justice Department), the United States Coast Guard (part of DHS as of 2003), the State Department's Bureau of Intelligence and Research, and the intelligence agencies of the Energy and Treasury departments.

These 14 organizations work separately and together in fulfillment of a number of functions. Their "customer base" includes the president, the NSC, and other officials of the executive branch. In meeting the needs of these

The Central Intelligence Agency "Fusion Center," a command and control office where action against terrorists is coordinated. ©ROGER RESSMEYER/CORBIS.

"customers," the IC produces and disseminates a variety of intelligence gathered through the four traditional methods of intelligence collection: human, signals, imagery, and measurement and signatures intelligence (HUMINT, SIGINT, IMINT, and MASINT respectively).

Intelligence collection is directed toward information on international terrorist and narcotics trafficking activities, as well as other hostile activities against the United States by foreign powers, organizations, persons, and/or their agents. Other areas of interest for the IC, and for the intelligence and security apparatus as a whole, include information on cyber warfare, threats to critical infrastructure, weapons of mass destruction, and international organized crime. Members of the IC are also, of course, involved in the conduct of "special activities," to use the IC term, which can and do involve covert action against entities deemed a threat to national security.

CIA and DCI. The modern security and intelligence apparatus had its beginnings after World War II, specifically with the National Security Act of 1947, which created CIA, DOD, and the NSC. Today the head of the CIA, the Director of Central Intelligence (DCI), also serves as principal intelligence advisor to the president, as well as director of the IC. He is also responsible for presenting the president with the annual IC budget, which must win congressional approval.

Staff organizations outside the CIA, but under DCI control, include the National Intelligence Council, responsible for preparing national intelligence estimates, and the Community Management Staff, which assists DCI in his IC executive functions. DCI also chairs two advisory boards, the National Foreign Intelligence Board and the Intelligence Community Executive Committee.

The CIA is an independent government organization tasked with supporting the president, the NSC, and other members of the national security leadership by providing accurate, comprehensive, and timely foreign intelligence on national security topics. CIA also supports the Chief Executive and other officials by conducting counterintelligence operations, "special activities," and other duties relating to foreign intelligence and national security as directed by the president.

The CIA includes four directorates: Operations, responsible for collecting foreign intelligence, including HUMINT, and for overseeing the overt collection of intelligence domestically through persons or organizations who volunteer that information; Intelligence, which produces the bulk of CIA's finished intelligence, processed from raw data collected in the field; Administration, which provides

support to CIA activities through a number of administrative and technical offices; and Science and Technology, which also provides support, through research, development, acquisition, and operations of technical capabilities and systems.

Defense Department

The vast Department of Defense, with its 3.2 million people (including active military, reservists, National Guard, and civilian personnel) includes several groups within the Intelligence Community, but a much greater portion of DOD lies outside the IC, with activities that fall under the heading of "security" rather than intelligence.

Among the key DOD components of the IC is the ultrasecret NSA, the nation's leading cryptologic organization, whose activities include eavesdropping and surveillance. Within it is the even more secretive Special Collection Service. NIMA and NRO are likewise secretive and concerned with surveillance, primarily through satellites. In fact, NRO's existence was not even known until 1992.

Additionally, DOD houses DIA and the intelligence services of the armed forces. Intelligence functions within the military services include the Army Intelligence and Security Command (INSCOM); the various organizations under the Air Combat Command; and the National Maritime Intelligence Center, which houses the intelligence activities of the Navy, Marine Corps, and Coast Guard. (The last of these, in wartime, is attached to DOD rather than DHS.)

Unified commands and defense agencies. In addition to the services, DOD is divided into nine unified commands. Among the latter are five with geographic areas of responsibility, and four with non-geographic areas of focus. These are the Joint Forces Command, concerned with training and new solutions to future challenges; Strategic Command, which controls missile, deterrence, space, and satellite systems; Special Operations Command, which comprises a number of special support teams, including the Navy SEALs, Army Special Forces, and Delta Force; and the Transportation Command, responsible for moving personnel and materials around the world.

DOD also includes 15 defense agencies, many of which are critical to national security. These include not only DIA, NIMA, and NSA, but also the Defense Security Service, Defense Security Cooperation Agency, Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Information Systems Agency, and Missile Defense Agency.

Justice, Treasury, and other Departments

A number of components of CIA are concerned with counterintelligence, or the use of intelligence resources to identify, circumvent, and neutralize the intelligence activities of a foreign power. Likewise, the FBI has a major counterintelligence unit, the National Security Division. The FBI as a whole is concerned not just with federal law enforcement in the United States, but with intelligence-gathering in the Western Hemisphere.

In addition to the FBI, the Justice Department contains a number of other components involved with intelligence and security, among them the Drug Enforcement Administration (DEA), the National Drug Intelligence Center (NDIC), and the U.S. National Central Bureau, which coordinates with Interpol. As of 2003, Justice was also home to the Bureau of Alcohol, Tobacco, Firearms, and Explosives, formerly a part of Treasury.

The latter department remains home to a number of agencies concerned with the security of financial assets, and with intelligence regarding financial activities. Treasury intelligence functions are a part of the IC. The Commerce Department, though it has no IC members, contains a number of organizations concerned with intelligence or security, most notable among them being the Critical Infrastructure Assurance Office.

State, Energy, Transportation, and Homeland Security

Among the State Department offices involved in the IC are the Bureau of Intelligence and Research, the Bureau for International Narcotics and Law Enforcement Affairs, the Office of the Coordinator for Counterterrorism, the Foreign Emergency Support Team, and the Bureau of Diplomatic Security. The Energy Department is inherently concerned with national security, inasmuch as it protects U.S. energy resources, and within it are intelligence components that belong to the IC. Most of these are part of the National Nuclear Security Administration, which is charged with protecting U.S. nuclear materials.

The Transportation Department houses the Federal Aviation Administration, which has had a particularly important function in national security since the terrorist attacks of September 11, 2001. Transportation was also briefly home to the Transportation Security Administration, which oversees airport security screeners and air marshals, but those functions were moved to DHS. The latter includes a number of other agencies that formerly belonged to other departments, among them the U.S. Secret Service, Customs Service, Immigration and Naturalization Service, Border Patrol, and the Federal Law Enforcement Training Center.

Independent agencies. Among independent agencies, GSA plays a role in the security of federal buildings, many thousands of which it manages. This role has been particularly critical since the terrorist bombings in Oklahoma

City in April 1995. GAO studies the efficiency of U.S. activities and accounts for expenditures. It issues some 1,000 reports a year, and since September 2001, its evaluations of security measures undertaken by the federal government have provided a key means for assessing the degree to which various agencies and departments are prepared—or not prepared—for terrorist threats.

FEMA and the EPA work with a number of agencies, including the Coast Guard, to respond to emergencies involving environmental hazards and similar threats. The United States has a number of entities concerned with emergency response, many of which work with state and local authorities. EPA and the Coast Guard co-chair the U.S. National Response Team, an interagency group charged with emergency response planning and coordination. In times of emergency involving threats to health, the Public Health Service is additionally a key component of the national response.

FURTHER READING:

BOOKS:

Jeffreys-Jones, Rhodri. *Cloak and Dollar: A History of American Secret Intelligence.* New Haven, CT: Yale University Press, 2002.

Johnson, Loch K. *Secret Agencies: U.S. Intelligence in a Hostile World.* New Haven, CT: Yale University Press, 1996.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

ELECTRONIC:

U.S. Intelligence and Security Agencies. Federation of American Scientists. <http://www.fas.org/irp/official.html> (April 29, 2003).

U.S. Intelligence Community. <http://www.intelligence.gov/> (April 14, 2003).

SEE ALSO

Air Force Intelligence, United States
Air Force Office of Special Investigations, United States
Air Marshals, United States
Arms Control, United States Bureau
ATF (United States Bureau of Alcohol, Tobacco, and Firearms)
Aviation Security Screeners, United States
Chemical and Biological Defense Information Analysis Center (CBIAC)
CIA (United States Central Intelligence Agency)
Civil Aviation Security, United States
Coast Guard (USCG), United States
Coast Guard National Response Center
Commerce Department Intelligence and Security Responsibilities, United States
Communications System, United States National
Coordinator for Counterterrorism, United States Office
Counter-Intelligence
Critical Infrastructure Assurance Office (CIAO), United States
Customs Service, United States
DCI (Director of the Central Intelligence Agency)
DEA (Drug Enforcement Administration)
DARPA (Defense Advanced Research Projects Agency)
Defense Information Systems Agency, United States
Defense Security Service, United States
Department of State Bureau of Intelligence and Research, United States
Department of State, United States
DIA (Defense Intelligence Agency)
Diplomatic Security (DS), United States Bureau
DOD (United States Department of Defense)
DOE (United States Department of Energy)
Domestic Emergency Support Team, United States
Drug Control Policy, United States Office of National
FEST (United States Foreign Emergency Support Team)
FAA (United States Federal Aviation Administration)
FBI (United States Federal Bureau of Investigation)
Federal Protective Service, United States
Foreign Assets Control (OFAC), United States Office
General Services Administration, United States
Homeland Security, United States Department
Information Security (OIS), United States Office
Infrastructure Protection Center (NIPC), United States National
INSCOM (United States Army Intelligence and Security Command)
Inspector General (OIG), Office of the
Intelligence Community
Intelligence Policy and Review (OIPR), United States Office
Intelligence Support, United States Office
Intelligence, United States Congressional Oversight
International Narcotics and Law Enforcement Affairs (INL), United States Bureau
Interpol (International Criminal Police Organization)
Justice Department, United States
Law Enforcement Training Center (FLETC), United States Federal
Military Police, United States
National Archives and Records Administration (NARA),United States
National Response Team, United States
NIC (National Intelligence Council)
NSC (National Security Council)
Navy Criminal Investigative Service (NCIS)
NCIX (National Counterintelligence Executive), United States Office of the
NDIC (Department of Justice National Drug Intelligence Center)
NFIB (United States National Foreign Intelligence Board)
NIMA (National Imagery and Mapping Agency)
NIST (United States National Institute of Standards and Technology)
NIST Computer Security Division, United States
NMIC (National Maritime Intelligence Center)
National Military Joint Intelligence Center
NNSA (United States National Nuclear Security Administration)
NRO (National Reconnaissance Office)
NSA (United States National Security Agency)
Nuclear Emergency Support Team, United States
PFIAB (President's Foreign Intelligence Advisory Board)
President of the United States (Executive Command and Control of Intelligence Agencies)
Public Health Service (PHS), United States
Secret Service, United States
Security Policy Board, United States

Security, Infrastructure Protection, and Counterterrorism, United States National Coordinator
Soldier and Biological Chemical Command (SBCCOM), United States Army
Special Collection Service, United States
Special Operations Command, United States
Surgeon General and Nuclear, Biological, and Chemical Defense, United States Office
Terrorist Organization List, United States
Transportation Department, United States
Treasury Department, United States
USAMRICD (United States Army Medical Research Institute of Chemical Defense)
USAMRIID (United States Army Medical Research Institute of Infectious Diseases
USSTRATCOM (United States Strategic Command)

United States Intelligence, History

MICHAEL J. O'NEAL

From its inception, the United States made use of spies. The nation's first spymaster, General George Washington, recognized the need for accurate intelligence during the Revolutionary War. In a letter written July 26, 1777, Washington wrote: "The necessity of procuring good intelligence is apparent & need not be further urged—All that remains for me to add is, that you keep the whole matter as secret as possible." From his experience as a British officer in the French and Indian war, he often relied on intelligence provided by Native Americans to keep his troops mobile and out of reach of the enemy.

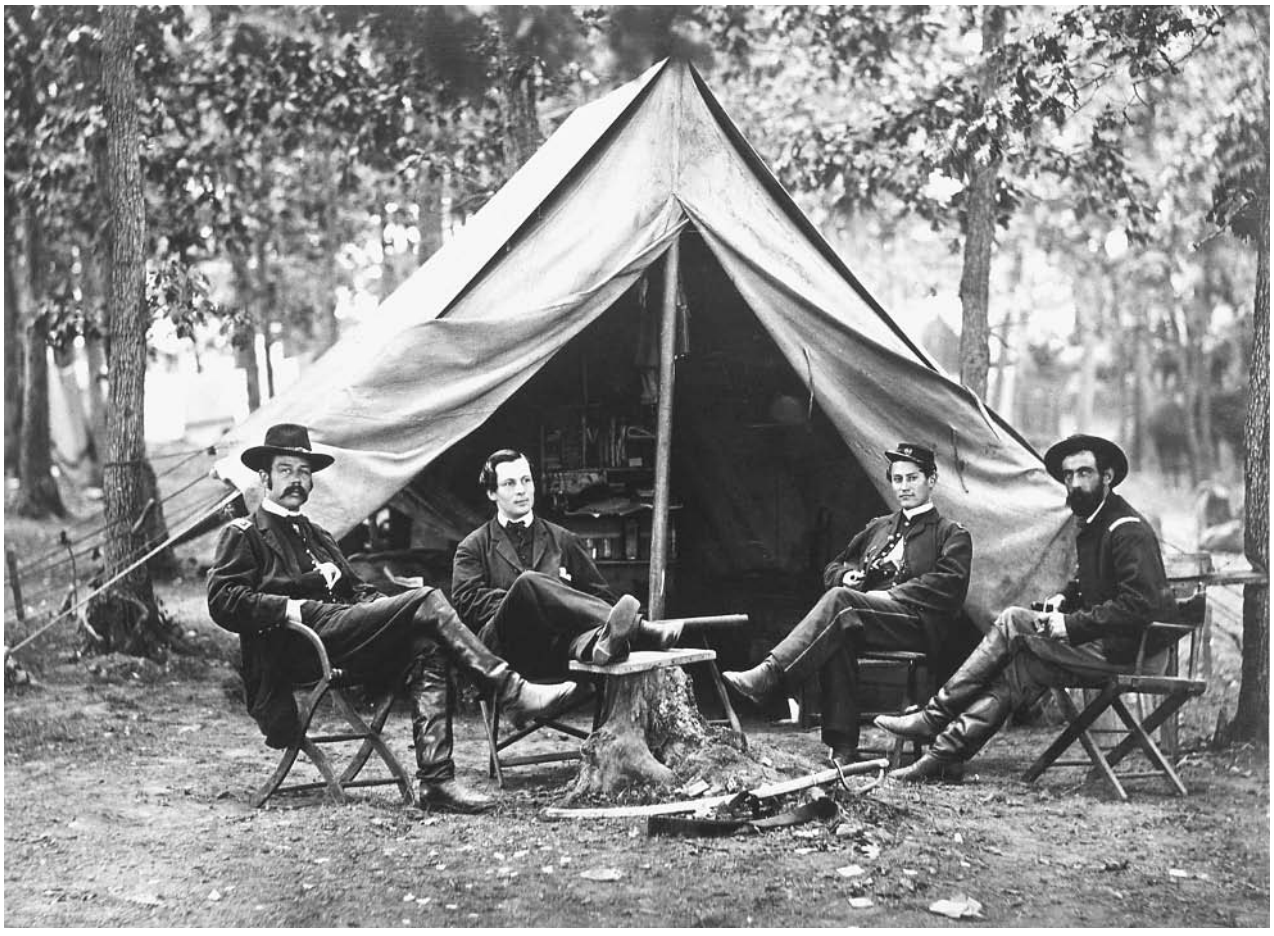
Intelligence operations in the American colonies, though, predate the war. In 1765, after the British passed the hated Stamp Act, a confederation of dissident groups called the Sons of Liberty formed to harass the British. By 1772 the Sons of Liberty had evolved into the Committees of Correspondence, whose purpose was to share information in resisting colonial rule. In Boston, members of the committee, including Samuel Adams and John Hancock, patrolled the streets at night, observing the movement of British troops and warning rebels in the countryside of impending British raids that might turn up caches of arms and gunpowder. The Boston group learned that on one of these raids the British intended to arrest Adams and Hancock, but it was unclear whether troops leaving Boston would travel across land or up the seacoast. In an early instance of intelligence tradecraft, Paul Revere arranged a signal that would give the rebels in the countryside advance warning of the direction of the raid—lanterns hung in the steeple of Boston's Old North Church. His stratagem, "one if by land, two if by sea," was immortalized by Henry Wadsworth Longfellow in his poem *Paul Revere's Ride*. This raid went down in the history books as the Battles of Lexington and Concord, the opening salvos in the Revolution.

The Revolution also produced the new nation's first intelligence "mole" and the nation's first cryptanalyst. The mole was Dr. Benjamin Church, who posed as a member of the Boston group while secretly providing intelligence about American rebel activities to General Thomas Gage, commander of the occupying British troops in Boston. Later, as chief surgeon of the Continental Army, Church continued to funnel information to the British. He was finally exposed through a compromising letter he wrote in code. The letter eventually fell into the hands of Washington, who hired an amateur cryptanalyst, the Reverend Samuel West, to decipher it. Church was sent into exile and never heard from again.

Even Benjamin Franklin took part in spy games as head of the nation's first formal intelligence-gathering organization, the Committee of Secret Correspondence. Formed in 1775, the committee's principal goal was to gather information about sentiments toward the Revolutionary War in Europe. Franklin secretly negotiated with European powers to purchase arms and supplies. He also negotiated with France to procure the aid of French troops, whose arrival broke the war's stalemate and ultimately turned the tide in favor of the colonists.

In the decades following the Revolution, Americans adopted an isolationist stance and were absorbed with the task of building a nation, so they saw little need to take part in international espionage or to defend against it. As a result, the nation had few secrets, and the French, British, and Spanish in particular had little trouble learning American intentions. As tensions mounted again between Great Britain and the United States before the War of 1812, the British had secret agents throughout the country and even in the government itself. For its part, U.S. intelligence was so feeble that troops did not even have accurate maps of U.S.-Canadian border areas, the staging ground for British attacks. Even when U.S. authorities did acquire intelligence information, no one knew what to do with it. They knew, for example, that the British intended to burn Washington, D.C. No steps were taken to protect the capital.

The Civil War. Intelligence operations during the Civil War are wrapped today in an aura of romantic myth, perhaps because they represent the apex of the amateur spy. Legends in particular surround the efforts of women spies who often, according to legend, galloped across borders on horseback in the moonlight carrying to their brave men information concealed in their bodices. At the war's start, President Abraham Lincoln knew virtually nothing about the South's war-making capabilities. To gather intelligence, he, like Washington, became his own spymaster, running such men as William Alvin Lloyd, a transportation expert and publisher who moved freely about the South and provided valuable information about Southern troop



These officers with the Secret Service Department managed scouts and spies attached to the Army of the Potomac during the Civil War. ©CORBIS.

movements and the fortifications around cities like Richmond, Virginia. As an amateur, though, Lloyd developed no way to pass information in secret, and he even carried much of the information he gathered about with him on his person.

In the North, two rival intelligence organizations formed. One was run by the famous detective Allan Pinkerton, who reported to General George McClellan, commander of the Army of the Potomac. The other was headed by Lafayette Baker, who reported to General Winfield Scott and later to the secretary of state. These rival organizations often worked at cross-purposes, on occasion even arresting one another's members. While they frequently unearthed valuable information about Southern troop movements, officers assigned to intelligence work lacked experience and there was little coordination of their efforts. Too frequently, Northern commanders failed to act on the information they received.

The South, meanwhile, carried on widespread intelligence operations against the North, although again it is difficult to separate fact from fiction because when Richmond, the Confederate capital, fell, virtually all records of their operations were destroyed. Thus it remains an open question, for example, whether John Wilkes Booth, Lincoln's assassin, was on the Confederate payroll as a spy. As an actor, he traveled freely throughout the cities of the North, giving him ample opportunity to meet with members of the network of spies the South had placed in New York City, Baltimore, Washington, Philadelphia, and other cities. In 1864 he played several engagements in Niagara Falls, New York, a hotbed of Southern espionage just over the border from Montreal. Montreal was the headquarters of the "Canadian Cabinet," a group of Southern leaders who directed espionage operations against the North. After fires broke out in several New York City hotels on November 25, 1864, a captured Southern agent confessed that the fires were the work of the Canadian Cabinet. Booth, it turned out, had been in Canada in the days preceding the arson raid and had met with the cabinet. Further, one of Booth's co-conspirators in the Lincoln assassination was John Surratt, a known Confederate spy and gun runner whose mother, Mary Surratt, was later hanged for her role in Lincoln's death.

The beginnings of professional intelligence. In the decades between the Civil War and World War I, the United States

took its first faltering steps toward development of an organized, professional intelligence capability. In 1885, President Grover Cleveland called for assignment of military attachés to foreign countries to gather information. During the Spanish-American War of 1898, the United States acquired—and most importantly, acted upon—human intelligence about Spain's war-making capabilities. John Wilkie, head of the U.S. Secret Service, broke up the "Montreal spy ring" Spain had put in place in Canada. Before and during American participation in World War I, counterintelligence agents of the FBI and Secret Service were successful at ferreting out German agents and saboteurs within the United States, but during the war, the nation relied on cooperative arrangements with the British for overseas intelligence. It was the British, for example, who broke German diplomatic codes and in 1917 intercepted and deciphered the infamous Zimmermann telegram revealing Germany's intention to begin unrestricted submarine warfare against the United States.

Between the two world wars, American intelligence again fell into abeyance. Typically, only inexperienced officers with little or no training in intelligence were sent to staff foreign embassies, so little valuable intelligence about Soviet, German, and Japanese intentions was acquired on the ground. Most U.S. intelligence was directed internally against radicals, subversives, communists, and anarchists during the "Red Scare" of the 1920s and against Nazi agents in the 1930s. The United States did, however, make strides in code breaking and began to develop an organized intelligence capability. In 1922, William Friedman, a Russian immigrant, was appointed chief cryptanalyst of the Army Signal Intelligence Service (SIS), which broke the Japanese Purple code, the principal cipher Japan used to send diplomatic messages as tension between the United States and Japan mounted. After the Japanese attack on Pearl Harbor on December 7, 1941, U.S. intelligence efforts focused on cracking Japan's code for transmitting military messages. Leading the effort, code-named "Magic," was the U.S. Navy's Combat Intelligence Unit. Using complex mathematical analysis, IBM punch-card tabulating machines (the first example of cooperation between the military and private enterprise to gather intelligence), and a cipher machine, the unit was able to crack the code. Throughout World War II, the United States intercepted and decoded thousands of Japanese communications; cryptanalysts gave U.S. war planners advance notice of Japanese plans to attack Midway Island in June 1942, allowing U.S. forces to lie in wait, defeat the Japanese, and turn the tide in the Pacific.

Modern U.S. intelligence. The chief deficiency of U.S. intelligence during World War II was that it was scattered among the various branches of the military; whatever coordination it received happened only on President Franklin Roosevelt's desk. To correct this deficiency, Roosevelt appointed William J. Donovan, a New York lawyer and former Army colonel, to assemble a plan for an intelligence service. Out of Donovan's plan emerged the Office of Strategic Services (OSS) in June 1942. Under Donovan's leadership, the OSS was given the task of collecting and analyzing information needed by the Joint Chiefs of Staff and to conduct "special operations," or clandestine operations that were not carried out by other federal agencies or the military. Throughout the war the OSS provided policy makers and the military with enemy troop strength estimates and other intelligence that was crucial to planning military campaigns.

The cold war with the Soviet Union following World War II gave increased urgency to the need for good intelligence, but opinion was divided about who should conduct intelligence operations and who should supervise their efforts. Roosevelt's successor, Harry S. Truman, divided responsibilities between military and civilian agencies in October 1945 when he abolished the OSS and transferred its operations to the Departments of War and State. Donovan, though, favored the formation of a strictly civilian organization that would coordinate intelligence gathering. Fearing that the plan would lessen their influence, both the military and the FBI opposed it. Truman struck a middle course in January 1946 when he established the Central Intelligence Group (CIG), giving it the authority to coordinate intelligence gathered by existing departments and agencies. The CIG was placed under the supervision of a National Intelligence Authority, which consisted of the president and the secretaries of the State, War, and Navy departments. Thus, for the first time in its history the United States had a peacetime intelligence organization. Less than two years later, though, Congress passed the 1947 National Security Act, creating the civilian National Security Council (NSC) and placing under its authority the Central Intelligence Agency (CIA). Intelligence gathering was now firmly under the control of civilian rather than military authorities.

In the 1950s and early 1960s the CIA was the nation's bulwark against the expansion of communism and Soviet influence. It was the CIA, for example, that revealed the presence of Soviet missiles in Cuba during the 1962 Cuban Missile Crisis. Its reputation was tarnished, though, by the disastrous Bay of Pigs operation against Cuban dictator Fidel Castro and reports of unsavory CIA activity during the war in Vietnam and, in the 1970s and 1980s, against unfriendly leftist regimes in Central and South America. After the terrorist attacks of September 11, 2001, the CIA took on added luster as the nation looked to it as the front line in the fight against terrorism.

In its early years the CIA relied primarily on human intelligence and field operations. Its science and technology efforts were scattered among various CIA divisions, or "directorates." With the success of overhead intelligence-gathering technology, including the U2 spy plane and reconnaissance satellites, then CIA director John McCone wanted to gather all of the agency's scientific and technological capabilities under one roof. The result was the formation of the Directorate of Science and Technology (DS&T) in 1963. Throughout its history, the DS&T has

enjoyed numerous successes, developing high-tech imagery and eavesdropping satellites and a host of other sophisticated tools that have proven invaluable in acquiring information while keeping American operatives out of harm's way.

■ FURTHER READING:

BOOKS:

Andrew, Christopher. *For the President's Eyes Only: Secret Intelligence and the Presidency from Washington to Bush.* New York: Harper Perennial, 1995.

Kahn, David. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* New York: Scribner, 1997.

Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence.* New York: Paragon House, 1989.

O'Toole, G. J. A. *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA.* New York: Atlantic Monthly Press, 1991.

Richelson, Jeffrey T. *A Century of Spies: Intelligence in the Twentieth Century.* New York: Oxford University Press, 1995.

SEE ALSO

CIA, Formation and History
CIA Directorate of Science and Technology (DS&T)
Civil War, Espionage and Intelligence
Cryptology, History
Cuban Missile Crisis
Espionage and Intelligence, Early Historical Foundations
National Security Act (1947)
NSC (National Security Council), History
Pearl Harbor, Japanese Attack on
Revolutionary War, Espionage and Intelligence
Spanish-American War
War of 1812
World War II, United States Breaking of Japanese Naval Codes

United States Oil Reserve.

SEE *Strategic Petroleum Reserve, United States.*

Unmanned Aerial Vehicles (UAVs)

■ K. LEE LERNER

Israel was the first nation to make significant use of unmanned reconnaissance drones in combat during operations in Lebanon in 1982. The United States forces began full deployment and use of unmanned aerial vehicles (UAVs) and related technology in the 1990s and UAVs—especially the Predator and Global Hawk—were extensively used by U.S. forces during Operation Enduring Freedom in Afghanistan and Operation Iraqi Freedom.

Tactical Uses of UAVs

UAVs can fly in areas where air supremacy is not complete or air defenses have not been fully suppressed. UAV craft can also operate in biologically or chemically contaminated areas. In addition, UAVS offer a chance to conduct battle damage assessments—critical for further mission planning—without further risk to pilots.

As of May 2003 more than 1500 UAV sorties had been flown in Afghanistan and UAV craft destroyed, or assisted in the destruction of, nearly a thousand targets. In addition to the capability of some UAVs to fire Hellfire missiles, UAV can paint targets with lasers that guide other weapons systems.

UAV Capabilities

The Predator flies at medium altitudes and is capable of long reconnaissance and surveillance missions. In conjunction with weapons systems, Predator craft are also used for target acquisition.

The Global Hawk, is capable of operating at higher altitudes (in excess of 60,000 ft) on and features an integrated sensor system that enhance its intelligence, surveillance, and reconnaissance capabilities.

The U.S. Navy operates the Pioneer UAV. Designed to operate over open ocean, the Pioneer design incorporates a low radar cross section and reduced infrared signature. Pioneer craft were first used during operations in Grenada and strikes against Libya.

The Shadow UAV offers day and night surveillance capability and can carry a 330 lbs. Payload while operating at 10,000 ft. The U.S. Army uses Shadow UAVs to call in or lock on (calibrate) artillery attacks.

UAV use has also spurred advances in miniaturized synthetic aperture radar that reduces weight but still offers high stationary and moving target resolution (i.e. radar that can discriminate targets separated by less than 18 inches (.5 m).

UAVs as platforms for weapons of mass destruction or terrorism. Prior to its being eliminated by U.S. forces, U.S. officials claimed that Saddam Hussein's Iraqi regime had developed and tested a limited number of UAVs capable of delivering biological agents.

In 2003, Hamas operatives were killed as they were preparing to test an unmanned aerial vehicle (UAV) purchased from illegal arms dealers. The craft exploded before Hamas could carry out a planned attack against a

The U.S. military used several unmanned spy aircraft such as this GNAT Aerial Reconnaissance Vehicle to help the Philippine military hunt down Islamist extremist guerrillas on the Philippine island of Basilan in 2002. AP/WIDE WORLD PHOTOS.

target inside Israel. Hamas spokesmen subsequently claimed that they been fooled into purchasing a booby-trapped UAV by the Israeli Security Agency ISA (Shin Bet).

Western press organizations have also carried reports that Palestinian agents have attempted purchases of model aircraft from suppliers in Europe with the intent to develop a crude but UAV capability. One factor limiting these types of operations is that typical hobbist UAVs require line-of-sight control of the aircraft and are therefore incapable of navigating with precision over rugged terrain or over great distances.

UAV use in intelligence operations and current research. In November, 2002, a CIA-operated Predator operating over Yemen fired a missile that killed bin Laden's top lieutenant in Yemen, Qaed Salim Sinan al-Harethi, and five other al-Qaeda suspects.

DARPA planned advancement of the Unmanned Combat Air Vehicle (UCAV) and Unmanned Combat Armed Rotorcraft (UCAR) is designed to enhance the ability to remotely suppress enemy air defenses, conduct extended surveillance in hostile territory, and pursue armed reconnaissance and attack missions.

A milestone in unmanned aviation, in 2002, the U.S. flew an unmanned plane on a trans-Pacific flight from California to Australia.

DoD and Northrop Grumman engineers are currently refining the Eurohawk for advanced electronics and signals intelligence operations. France is developing the Système de Drone Tactique Interimaire (SAGEM) and United Kingdom is developing a craft termed "Watchkeeper" to replace the Phoenix.

FURTHER READING:

ELECTRONIC:

Airborne Autonomous Systems. Unmanned Aircrft.<http://www.unmannedaircraft.com/> (May 12, 2003).

American Forces Press Service, Garamone, Jim. "From U.S. Civil War to Afghanistan: A Short History of

UAVs." April, 16, 2002. <http://www.defenselink.mil/news/Apr2002/n04162002_200204163.html> (May 12, 2003).

SEE ALSO

Aviation Intelligence, History
Balloon Reconnaissance, History
Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)
Persian Gulf War
Weapons of Mass Destruction, Detection

UNSCOM (United Nations Special Commission).

SEE *Iraq War: Prelude to War (The International Debate Over the Use and Effectiveness of Weapons Inspections.)*

Uranium

LARRY GILMAN

Uranium is a radioactive, metallic element with 92 protons and a variable number of neutrons in the nucleus of each atom. There are 16 isotopes of uranium, the most common being uranium-238 (^{238}U). The second-commonest isotope of uranium, ^{235}U, is used for building nuclear weapons, generating electricity, and propelling some submarines, aircraft carriers, and other vessels. Heat released by uranium decay also keeps Earth's interior hot, providing the energy for continental drift and volcanic eruptions.

Uranium was discovered in 1789 by German chemist Martin Heinrich Klaproth (1743–1817), and its property of radioactivity was discovered by French physicist Henri Becquerel (1852–1908) in 1896. ^{235}U was first isolated in kilogram quantities by the United States during World War II, and was used in war by the United States in the bomb that destroyed the city of Hiroshima, Japan in 1945. Since that time uranium has been mined in many countries and purified in large quantities for both bombs and fuel. Worldwide, several hundred nuclear reactors produce electricity from uranium, while tens of thousands of nuclear weapons (mostly held by the United States and the Russian Federation) rely on uranium either as their primary explosive (in fission bombs) or as a trigger explosive (in fusion bombs).

Uranium atoms are unstable; that is, their nuclei tend spontaneously to fission or break down into smaller nuclei, fast particles (including neutrons), and high-energy photons. The fission of an isolated uranium nucleus is a randomly timed event; however, collision with a neutron may trigger a uranium nucleus to fission immediately. Crowding large numbers of uranium atoms together can enable the neutrons emitted by a few nuclei undergoing fission to cause other nuclei to fission, whose released neutrons in turn trigger still other nuclei, and so on. If this chain reaction proceeds at a constant rate, it may be used to generate electricity; if it proceeds at an exponentially increasing rate, a nuclear explosion results.

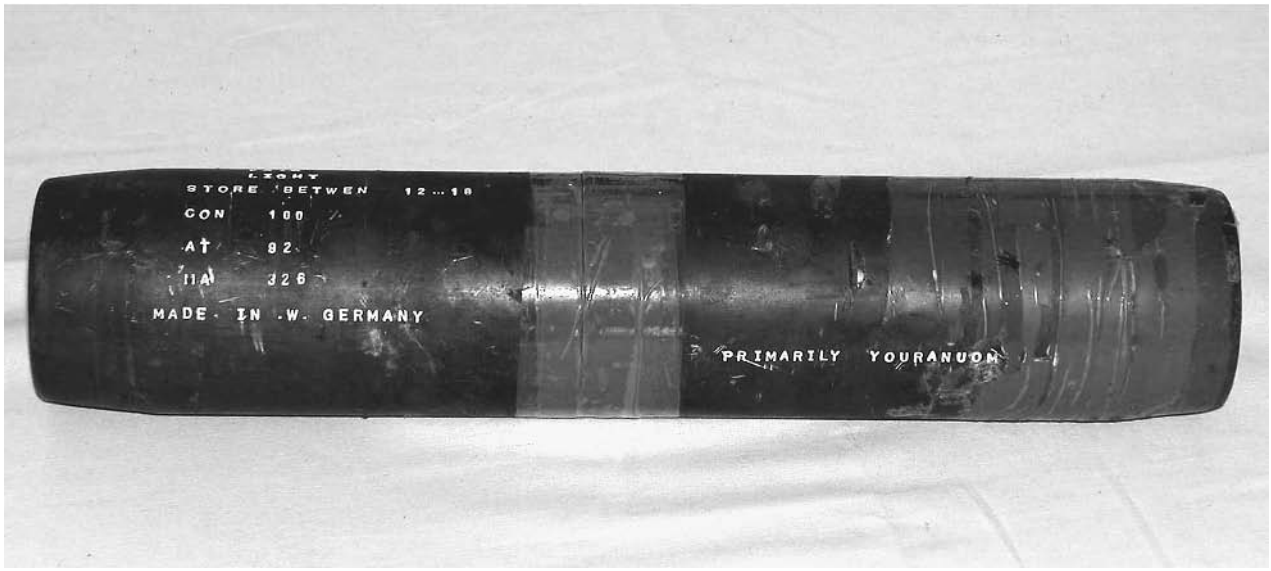
Only 0.71% of natural uranium is ^{235}U, the major isotope directly useful for nuclear power and weapons. Many tons of ore must therefore be refined to produce a single kilogram of ^{235}U. The amount of ^{235}U needed to make a bomb, however, is not great: about 15 lb (7 kg). Quantities of uranium sufficient for many thousands of bombs are thus available around the world; some 21 countries export uranium, with Canada, Australia, and Niger being the three largest producers.

The most common isotope of uranium, ^{238}U, comprises 99.28% of the uranium in the Earth's crust. ^{238}U is comparatively stable, with a half-life of 4.5 billion years, and so is not directly useful for power and nuclear weapons. It is added to some antitank and antiaircraft ammunition to increase their density and thus their penetrating power. Depleted-uranium munitions, as these weapons are termed, were used extensively by the United States during the Gulf War of 1991 and in the Kosovo conflict of 1999. Because of their slight radioactivity, there is ongoing debate about whether they may cause long-term health problems in areas where they have been used.

^{238}U is also a major ingredient of most reactor fuel. In reactor cores, this ^{238}U is bombarded by neutrons, which transmute some of it into the element plutonium. Plutonium can be used directly for power and weapons; the first and third nuclear weapons ever exploded were produced by the United States using plutonium transmuted from ^{238}U, and a number of other countries, including India, Israel, Pakistan, and North Korea, have developed the capability to obtain plutonium for bombs by the same means.

Both ^{235}U and plutonium must be in fairly concentrated form for use in bomb manufacture. Alloys that have been diluted by ^{238}U or other substances result in bulkier explosive devices; at sufficiently great dilution, a nuclear explosion is not obtainable. (However, some experts say that a nuclear explosion might be obtainable from an alloy that is as little as 10% ^{235}U.) It follows that any organization that wishes to build an atomic weapon must either obtain fairly concentrated ^{235}U or plutonium by purchase or theft, or obtain them in dilute form and then concentrate them.

These obstacles have been surmounted by a number of governments, and may eventually be surmounted by terrorist organizations. Illegal traffic in weapons-grade ^{235}U and plutonium has accelerated since the breakup of the Soviet Union in 1991, because its successor states have been too poor and disorganized to keep nuclear material secure. Some 600 tons, or enough for about 40,000 bombs, of raw weapons-grade fissionables are



Weapons-grade uranium, captured near the Syrian border at Sanliurfa, Turkey, in Septemebr 2002, is displayed at the Sanliurfa paramilitary police headquarters. AP/WIDE WORLD PHOTOS.

stored in poorly guarded stockpiles in the Russian Federation and other states; small quantities have already entered the black market. On over 16 occasions since 1993, police in Asia, Europe, or South America have intercepted illegally held bomb-grade uranium or plutonium, most of it from ex-Soviet sources. In 1994, police seized a metal briefcase when a civilian jetliner from Moscow landed in Munich, Germany; the briefcase contained 363.4 grams of weapons-grade plutonium. In April 2000, almost a kilogram of bomb-grade uranium was seized in the Republic of Georgia. In 2001, police in Bogota, Colombia seized some 600 grams of bomb-grade ^{235}U from the house of an animal feed salesman, the enrichment level of which corresponded to that of Russian fuel for submarines and icebreakers. And on September 11, 2001, four men were arrested in the ex-Soviet republic of Georgia in possession of almost 2 kilograms of bomb-grade ^{235}U—a large fraction of the amount required for a bomb. Since that day, the idea that stolen uranium might be used for terrorist acts has gained increased attention.

Through its Material Protection, Control, and Accounting Program, the United States has spent about $550 million since 1993 to help safeguard uranium and plutonium stocks in Russia, supplying complete security systems or partial protection for about a third of the material considered most vulnerable by the U.S. Department of Energy.

FURTHER READING:

PERIODICALS:

Ladika, Susan. "Tracing the Shadowy Origins of Nuclear Contraband." *Science* no. 5522 (2001): 1634.

Stone, Richard. "Nuclear Trafficking: 'A Real and Dangerous Threat'." *Science* no. 5522 (2001): 1632–36.

SEE ALSO

Nuclear Power Plants, Security
Nuclear Reactors
Nuclear Weapons

Uranium Depletion Weapons

LARRY GILMAN

Depleted uranium (DU) munitions are armor-piercing or general-purpose ammunition rounds that are composed, in part, of depleted uranium. Depleted uranium is uranium that has had most of its ^{234}U and ^{235}U removed for use in nuclear power or nuclear weapons, leaving metal that is almost entirely ^{238}U. ^{238}U is the least radioactive isotope of uranium, with a half-life of 4.46 billion years (6.3 times that of ^{235}U). It is used in munitions because of its density and hardness. The high density of DU (1.68 times that of lead, 2.43 times that of steel) allows it to transfer more kinetic energy to a target for a given round size than any other practically available metal. This, combined with its hardness, enables it to penetrate armor much more effectively than armor-piercing rounds made of other metals (e.g., tungsten). A typical armor-piercing DU round consists of a long, pointed shaft of DU that is surrounded by a sabot (from the French for "shoe"; a casing that fits the bore of the gun). When the round is fired, the sabot falls away, transferring some of its kinetic energy to the DU shaft.

When the shaft strikes end-on, its long, narrow shape concentrates all of the round's kinetic energy on a small area; as the round penetrates the armor it also tends, thanks to the particular mechanical properties of metallic uranium, to sharpen rather than to blunt or mushroom, further increasing its penetrating power.

DU is used not only for ammunition, but for ballast, gyroscope rotors, balancing weights on aircraft, armor enhancement, and in other applications calling for high-density material. The armor of the United States M1A1 Abrams Main Battle Tank, for example, consists of a layer of DU sandwiched between two layers of steel.

A variety of DU munitions have are in use by at least 20 technologically advanced military organizations around the world. The U.S. military leads both in quantities deployed and quantities used in combat. DU munitions were used by several branches of the U.S. military both in the Gulf War of 1991, in Bosnia-Herzegovina in 1994–95, and in Kosovo in 1999. During the Gulf War, U.S. forces fired 320 tons (290,300 kg) of DU munitions; during in Bosnia-Herzegovina, 3 tons (2721 kg); and in Kosovo, 10.2 tons (9253 kg). Much of this material remains on the ground.

There is no controversy about the military effectiveness of DU munitions. In an incident during the Gulf War, a U.S. Abrams tank with DU-enhanced armor was struck three times by main-gun rounds from three attacking Iraqi T-72 tanks. The Abrams remained operative despite the hits and responded with three DU main-gun rounds, destroying all three Iraqi tanks. Nevertheless, international debate has centered on the question of whether DU munitions pose a health hazard to military forces exposed to them during use or to civilian populations inhabiting regions contaminated by DU. There are two possible sources of health damage from DU: chemical toxicity and radioactivity.

Chemical toxicity. When a DU round strikes armor, it is pulverized and raised to a high temperature. Several oxygen-uranium compounds (uranium oxides) form under these conditions and can be harmful if inhaled or otherwise ingested (e.g., by direct penetration of the skin). Ingestion of sufficiently large quantities of uranium oxides can be harmful, especially to the kidneys. However, the U.S. government states that the quantities of uranium oxide that can be plausibly ingested under combat conditions, or by residents of contaminated areas, cannot be great enough to cause measurable health effects.

Radioactivity. The radioactivity of ^{238}U is very low compared to that of ^{235}U; further, although DU contains trace quantities of elements that are more radioactive, such as ^{235}U, americium, neptunium, plutonium, and technitium, these impurities increase DU's radioactivity by only about 0.8% over that of pure ^{238}U. Most scientists agree that the DU radiation hazard to troops and civilian populations in contaminated areas is too low to measure. Nevertheless, anecdotal reports of increased leukemia rates and other health problems in veterans exposed to DU have caused enough concern to trigger investigations of DU health effects by the United Nations Environmental Programme and several governments.

Although no ill effects from DU exposure have yet been definitely established by any study, the U.S. Department of Veterans Affairs is now tracking the health of veterans exposed to DU. Furthermore, the International Committee of the Red Cross has urged all countries that use DU munitions to review whether they comply with international agreements that forbid "weapons, means, or methods of warfare of a nature to cause superfluous injury or unnecessary suffering, which have indiscriminate effects, or which cause widespread, long-term and severe damage to the natural environment." Several such studies are now being pursued by European governments and by the U.S. government.

FURTHER READING:

ELECTRONIC:

Department of Defense Deployment Health Support Directorate. "Depleted Uranium Information Page." 2001. <http://www.deploymentlink.osd.mil/du_library/> (March 6, 2003).

International Committee of the Red Cross. "Depleted Uranium Munitions." June 6, 2001. <http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/57JR5D?OpenDocument> (March 6, 2003).

USAMRICD (United States Army Medical Research Institute of Chemical Defense)

The United States Army Medical Research Institute of Chemical Defense (USAMRICD) located in Aberdeen Proving Ground, Maryland, is a research and training laboratory dedicated to advancing the treatments that alleviate the suffering caused by chemical weapons and developing new materials that aid in those treatments. Researchers at the laboratory include experts in physiology, toxicology, pathology and biochemistry.

Established in 1922 as part of the Army Medical Department, the laboratory was responsible for treating chemical weapon casualties during World War I. In the 1960s the division was renamed the U.S. Army Biomedical Laboratory. The laboratory was put under the command of the U.S. Army Surgeon General in 1979 and received its

A research scientist processes anthrax samples that are thought to contain a significant aerosol and respiratory hazard. AP/WIDE WORLD PHOTOS.

current name in 1981. Today, the USAMRICD is one of six laboratories and institutes under the authority of the U.S. Army Medical Research and Materiel Command.

Researchers at the USAMRICD have made hundreds of contributions to the scientific literature and have produced technical bulletins on procedures for collecting, handling, shipping, and preparing samples of chemical agents. The laboratory also operates a chemical surety facility. Along with its research charge, the USAMRICD is also a training institution. The Chemical Casualty Care Division (CCCD) provides courses in the management and treatment of chemical weapons injuries to medical professionals. Courses are offered at the laboratory, at off-site locations and as computer-based training. Much of the educational and training work of the USAMRICD is done in partnership with the United States Army Medical Research Institute of Infectious Disease (USAMRIID) in Fort Detrick, Maryland, which is the Army's primary laboratory for research into biological warfare agents.

FURTHER READING:

ELECTRONIC:

United States Army <http://mrmc-www.army.mil/> (April 10, 2003).

United States Army Medical Research Institute of Chemical Defense <http://chemdef.apgea.army.mil/> (April 10, 2003).

SEE ALSO

Chemical Warfare
USAMRIID (United States Army Medical Research Institute of Infectious Diseases)

USAMRIID (United States Army Medical Research Institute of Infectious Diseases)

BRIAN HOYLE

USAMRIID is an acronym for the United States Army Medical Research Institute of Infectious Diseases. The facility is operated by the Department of Defense and serves as the country's principal laboratory for research into the medical aspects of biological warfare. Specifically, the facility aims to develop vaccines for infectious

diseases, other treatments such as drugs, and tests to detect and identify disease-causing microorganisms.

While developed for use in the laboratory, USAMRIID is mandated to explore the use of the treatments and tests in the real world of the battlefield. The research conducted at USAMRIID is defensive in nature. Infectious microbes are investigated only to develop means of protecting soldiers from the use of the microbes by opposition forces during a conflict.

The infectious disease research expertise at USAMRIID is also utilized to develop strategies and training programs to do with medical defense against infectious microorganisms. For example, the agency regularly updates and publishes a handbook that details the various medical defenses against biological warfare or terrorism. This handbook, now in its fourth edition, is available to the public.

While some of the research conducted at USAMRIID is classified, other research findings of the resident civilian and military scientists are used to benefit the larger public community. USAMRIID and its counterpart USAMRICD (U.S. Army Medical Research Institute of Chemical Diseases) trains more than 550 military medical personnel each year on biological and chemical defense measures. Furthermore, over 40,000 military and civilian medical professionals have attended an annual course on the Medical Management of Biological Casualties from 1999 to 2002.

History of the USAMRIID. The Office of the Surgeon General of the Army established USAMRIID on January 27, 1969. The facility replaced the U.S. Army Medical Unit (USAMU), which had been operating at the Fort Detrick, Maryland location since 1956. The USAMU had a mandate to conduct research into the offensive use of biological and chemical weapons. This research was stopped by U.S. President Richard Nixon in 1969. In 1971 and 1972, the stockpiled biological weapons were destroyed.

The defensive research that USAMU had been conducting, such as vaccine development, was continued by USAMRIID. In 1971, the facility was reassigned to the U.S. Army Medical Research and Development Command. Also in 1971, the centerpiece laboratory was completed. Construction of the high laboratory, which was designed to house and study highly infectious and dangerous microorganisms, cost $14 million.

Biocontainment capability. Laboratories have a rating system with respect to the types of microbes that can safety be studied. There are four levels possible. A typical university research lab with no specialized safety features (i.e., fume hood, biological safety cabinet, filtering of exhausted air) is a Biosafety Level 1. Progression to a higher level requires more stringent safety and biological controls. A Biosafety Level 4 laboratory is the only laboratory that can safely handle microbes such as the Ebola virus, *Bacillus anthracis* (the cause of anthrax), the Marburg virus, and hantavirus.

USAMRIID has a 10,000 square foot Biosafety Level 4 facility and 50,000 square feet of Biosafety Level 3. It is the largest high-level containment facility in the United States and is one of only three such units. The others are at the Centers for Disease Control and Prevention in Atlanta, Georgia, and San Antonio, Texas. A fourth level 4 laboratory is planned for the Rocky Mountain Lab in Hamilton, Montana.

Entry to the Level 4 area requires passage through several checkpoints and the keying in of a security code that is issued only after the person has been successfully vaccinated against the microorganism under study. All work in the level 4 lab is conducted in a pressurized and ventilated suit. Air for breathing is passed into the suit through a hose and is filtered so as to be free of microorganisms.

The USAMRIID facility also contains a Biosafety Level 4 patent ward. The ward can house people who have been infected during a disease outbreak or researchers who have been accidentally exposed to an infectious microbe. This ward was used in 1982 to care for two researchers from the Centers for Disease Control and Prevention who were exposed to rat blood contaminated with the virus that causes Lassa fever. The two researchers, along with three others thought to have been exposed to the virus remained in the containment ward until they were determined to be free of infection.

Equipment is also available that allows the Biosafety Level 4 conditions to be mimicked in the field. Thus, an infected person can be isolated at the site of an outbreak and transported back to Fort Detrick for medical treatment and study of the infection.

Research and other activities. The research staff at USAMRIID numbers over 500 people and includes physicians, microbiologists, molecular biologists, virologists, pathologists, and veterinarians. Among the support staff who assist the researchers are laboratory technicians who have volunteered to be test subjects during clinical trials of vaccines and drugs.

As of late 2002, USAMRIID scientists have the ability to rapidly identify approximately 85 infectious microorganisms. Work is underway to develop protection against 40 of the microbes. Vaccines are in various stages of development for 10 of the microbes including the highly infectious anthrax bacterium, and the Ebola and Marburg viruses.

Researchers and support staff can also respond to disease outbreaks. On short notice, teams can journey to the site of the infection to begin an investigation. This response is often conducted in conjunction with personnel from the Centers for Disease Control and Prevention. USAMRIID teams can also respond to combat. A portable laboratory to treat biological warfare casualties can be quickly set up near a battlefield.

One well-known USAMRIID response occurred in 1989, when an outbreak of an Ebola virus occurred at a primate holding facility in nearby Reston, Virginia. Some personnel even became infected with the virus, which was later determined to be a different variety from that which causes hemorrhagic Ebola fever in humans. The response of the USAMRIID personnel was subsequently detailed in best-selling books and inspired popular movies.

The facility has played an important role in several military campaigns. For example, it served as the medical support staging area for vaccines, drugs, and medical equipment during Operation Desert Storm and Desert Shield beginning in October 1990. During these campaigns, the threat of biological warfare, including the use of anthrax and *Clostridium botulinum* spores, was real. USAMRIID's expertise in treating these infections was invaluable to the troops who were sent to Saudi Arabia and Kuwait.

USAMRIID and domestic terrorism. In the aftermath of the September 11, 2001 terrorist attacks on targets in the United States, several letters containing anthrax spores were sent to various locations in the eastern United States via the United States Postal Service. The culprits have not been apprehended as of late 2002. Sequencing of the genetic material from the spores determined that the source of the anthrax was a strain of the microbe that had been developed in the USAMRIID labs in the 1980s. Whether the bacteria actually used in the incidents came from USAMRIID or from another lab that acquired the bacteria from USAMRIID has not been established.

Between September 11 and the following May, USAMRIID received 31,000 samples, an average of almost 4,000 per month, and performed over 260,000 tests. During normal times four to six samples are analyzed each month. Before September 11, the Special Pathogens Sample Test Laboratory had a staff of six. Since the crisis, a tenfold increase in staff members work around the clock.

■ FURTHER READING:

BOOKS:

USAMRIID *USAMRIID's Medical Management of Biological Casualties Handbook, Fourth Edition.* Fort Detrick, MD: U.S. Army Medical Research Institute of Infectious Diseases, 2001.

ELECTRONIC:

USAMRIID. "Welcome to USAMRIID." The U.S. Army Medical Research Institute of Infectious Diseases. Fort Detrick, MD. July 25, 2002. <http://www.usamriid.army.mil/>(25 November 2002).

SEE ALSO

Biocontainment Laboratories
Biological Weapons, Genetic Identification
United States, Counter-terrorism Policy
Vaccines

USS *Cole*

■ STEPHANIE WATSON

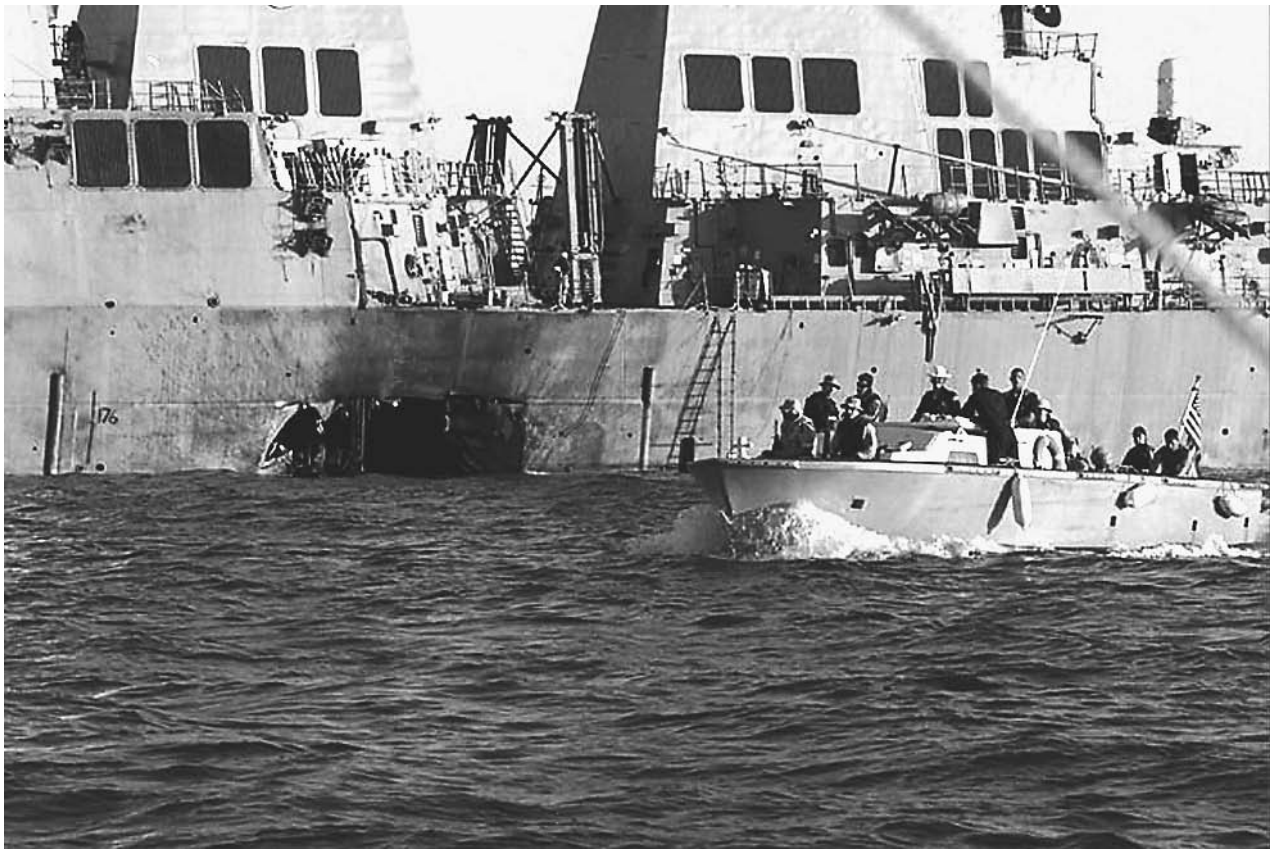
On the morning of October 12, 2000, as the Navy destroyer USS *Cole* sat anchored in the Yemeni port of Aden, a small boat packed with explosives rammed into its side, tearing a 40-foot hole through the ship's outer hull, killing seventeen sailors and wounding thirty-nine more. It was the deadliest attack against the United States military since 1996, when a truck bomb exploded near an apartment complex in Dhahran, Saudi Arabia, killing 19 American servicemen.

A ship in hostile waters. The *Cole,* one of the Arleigh Burke class of guided missile destroyers, was based in Norfolk, Virginia. The ship was on its way from the Red Sea to the Persian Gulf to help enforce United Nations sanctions against Iraq, when it made a routine stop in the Yemeni port of Aden for refueling. American intelligence officials had long been aware that Yemen was home to a number of Islamist fundamentalist groups. In the weeks before the attack, the country was home to violent demonstrations against the treatment of Palestinians in the Israeli-Palestinian conflict and America's supposed pro-Israeli stance. Although *Cole* Commander Kirk Lippold had been told of no specific threat against his ship, it was on what is known as "Threat Condition Bravo"—the second highest of four threat levels. At alerts of that level, the ship's guards were required to be on the lookout for small boats.

No flags were apparently raised when a small fiberglass boat approached the *Cole.* Eyewitnesses said the boat was helping the big destroyer with its mooring, when it pulled back to the *Cole's* port side. The two men on board reportedly stood at attention before their boat exploded, blowing a massive hole in the destroyer's steel hull. Damage to the $1 billion warship was estimated at $250 million.

Within hours of the explosion, Pentagon officials said they had reason to suspect a terrorist attack. FBI and CIA agents, as well as the Pentagon's Fleet Anti-Terrorist Support Team, were quickly sent to the scene to investigate. Within weeks, officials announced that they believed the blast to be the work of Osama bin Laden, the Saudi Arabian exile whose al-Qaeda terrorist network was also connected to the 1998 bombings of two American embassies in Kenya and the 1993 World Trade Center bombing. Al-Qaeda would later be linked to the September 11, 2001 attacks on the World Trade Center and Pentagon.

As the FBI and CIA began piecing together the evidence, they revealed that this wasn't the first plot against U.S. military interests in the region. Intelligence officials said they had already foiled at least two attempted plots against American ships. In mid-September 2000, a CIA report indicated the possibility that terrorists would attack a warship in the Mediterranean using a boat filled with



United States Navy and Marine Corps security personnel patrol past the damaged destroyer USS *Cole* following the October 12, 2000, terrorist bombing attack on the ship in Aden, Yemen. ©AFP/CORBIS.

explosives. And just two weeks before the attack, the Arab news channel Al Jazeera broadcast a video of bin Laden in which he made threats against the United States.

A troubled investigation. Although American intelligence officials moved quickly after the USS *Cole* attack, the investigation hit a number of snags. Yemeni officials questioned more than 1,500 people, yet they restricted American officials' access to key suspects. In June 2001, FBI agents were pulled out of Yemen because of credible evidence that there was a terrorist threat against them. The FBI and U.S. State Department disagreed over how to steer the investigation and deal with the uncooperative Yemeni government. The U.S. government still could not prove that al-Qaeda was behind the attack, and they were concerned that several key operatives remained at large, possibly planning more attacks against American interests.

United States officials did make significant progress in their investigation, eventually capturing several key suspects in the attack. In October 2002, the FBI nabbed a senior al-Qaeda operative named Abd Al-Rahim al-Nashiri, who is suspected of masterminding the *Cole* attack, as well as plotting several other attacks against other U.S. and British warships. The following month, a CIA-launched missile killed Abu Ali (also known as Qaed Senyan), a man who was said to have played a major role in the *Cole* attack, as he was traveling with five other al-Qaeda members in Yemen.

FURTHER READING:

PERIODICALS:

Hosenball, Mark, and Greg Vistica. "The Search for Clues: Did Officials Miss Hints of an Impending Attack?" *Newsweek.* November 6, 2000:45.

Kaplan, David E., Chitra Ragavan, and Richard J. Newman, et al. "Terror's Grim Toll." *U.S. News & World Report.* October 30, 2000:32.

MacLeod, Scott, Elaine Shannon, Mark Thompson, Edward Barnes, and William Dowell. "How Feuds and Culture Clashes Have Stymied the USS *Cole* Investigation." *Time.* Volume 158 (July 16, 2001): 38.

Nordland, Rod, John Barry, Mark Hosenball, Debra Rosenberg, and Gregory Vistica. "A Sneak Attack: Death at Sea." *Newsweek.* October 23, 2000: 27.

ELECTRONIC:

U.S. Department of State. "Attack on the USS *Cole:* IIP Archives." <http://usinfo.state.gov/topical/pol/terror/colearch.htm> (December 20, 2002).

SEE ALSO

FBI (United States Federal Bureau of Investigation)
Port Security

USS *Lapon*.

SEE *Undersea Espionage: Nuclear vs. Fast Attack Subs.*

USS *Liberty*

▮ ADRIENNE WILMOTH LERNER

The Liberty Incident refers to the June 8, 1967, attack on the United States intelligence ship *Liberty* by Israeli Defense Forces. The *Liberty* was stationed near the Sinai Peninsula and charged with monitoring Soviet communications to Soviet Arab allies during the Arab-Israeli Six Day War. Israeli troops reported they were taking fire from warships and deployed aircraft to find the source of enemy fire. The planes found the *Liberty* and fired upon the vessel. Torpedo boats also seized upon the *Liberty*. The attack killed 34 Americans, wounded 171, and destroyed the American ship. Israeli forces claimed that they had misidentified the *Liberty* as a hostile ship and attacked the vessel in error. Although the event sparked controversy, the attack was soon ruled an accident.

The USS*Liberty* was a World War II-era freighter built in 1945. The vessel sailed in post-war operations in the Pacific until it was retired in 1958. At the height of Cold War tensions, the National Security Agency (NSA) refitted several older military ships, turning them into intelligence vessels. The Liberty-class ships were designed to track radio signals and monitor communications between the Soviet Union and its allies. The *Liberty* itself measured over 450 feet long and carried a crew of 290 military and intelligence personnel.

The *Liberty*, like other ships in the intelligence fleet, was not constructed to be a warship. Navy and NSA officials assessed the risk of the ships encountering hostile forces was minimal, since all were to conduct operations only in international waters. The *Liberty* carried minimal defensive weapons, with only four .50 caliber machine guns mounted on the ship's deck. While the vessel was marked with its U.S. Navy identification number and flew an American flag, the ship maintained radio silence during most of its operations. Since the ships conducted operations in international waters, the American Navy rarely reported the position of its intelligence vessels to foreign intelligence services. Despite mission secrecy, the *Liberty*'s national origin and electronic surveillance capabilities could be ascertained by trained, careful observers.

The *Liberty*'s first mission as a refitted intelligence ship was monitoring radio communications off the coast of West Africa. As tensions grew between Israel and neighboring Arab nations, the *Liberty* was deployed to the eastern Mediterranean Sea. The vessel took on new personnel, including technical specialists and linguists trained in Russian and Arabic. However, no specially trained Hebrew language experts were assigned to the *Liberty*. The *Liberty* was stationed 13 miles off the Gaza coast, precariously close to Israel and Egypt, and in the middle of the developing conflict in the Middle East.

The presence of Soviet bombers in Alexandria strained U.S. relations with Egypt. As a result, diplomatic friendliness between Israel and the Unite States increased in an effort to halt Soviet backing of various Middle Eastern governments with military aid. The *USS Liberty*'s mission was to conduct remote intelligence, listening to radio transmissions, to ascertain the status of Soviet bombers and military officers in Egypt. As the ship began its mission, the Six-Day War erupted. Commander William McGonagle, Captain of the USS *Liberty*, requested a destroyer escort for his vessel, but the request was denied. Instead, U.S. Naval Command told McGonagle that jet fighter squadrons stationed on the island of Crete could provide rapid assistance if needed. A few hours later, U.S. Naval Command issued new orders to the *Liberty* to retreat further into international waters, 25 miles from the Sinai Peninsula. The *Liberty* never received the revised orders.

The *Liberty* remained in its location. Assured that the new orders had been received and heeded by the crew, U.S. military forces assured allies in the United Nations that no American vessels were present in the war area. On June 8, 1967, Israeli troops reported that they were being fired on from vessels at sea. Israeli intelligence deployed jet fighters to scout for Egyptian and other hostile boats in the region. Jet fighter scouts mistakenly reported to Israeli Defense Force Command that they located the Egyptian vessel, *El Quseir*, which had attacked Israel forces the day before. However, the planes actually reported the location of the USS *Liberty*, which they had misidentified.

Israeli forces swiftly attacked the *Liberty* with both jet fighters. The *Liberty* responded by turning its only weapons, the four .50 caliber machine guns, on the assaulting forces. The Israelis responded by launching napalm canisters and torpedoes from warships. The *Liberty* broke radio silence and tried to contact Israeli forces to identify the vessel as an American intelligence ship. However, Israeli forces had jammed the ship's communications systems with extensive static. Finding an open channel, *Liberty* communications officers radioed U.S. air forces in Crete for assistance. Receiving the distress call, jet fighters were deployed to aid the besieged *Liberty*. However, U.S. military officials recalled the planes after discovering that the jet fighters were not equipped to repel the attack. Without defensive weapons or fighting assistance, the *Liberty* was quickly crippled. Crewmembers later reported that Israeli

Israeli planes and one or more torpedo boats mistakenly attacked this U.S. Navy research ship, the USS *Liberty,* in the Mediterranean Sea near the Sinai Peninsula in 1967. ©BETTMANN/CORBIS.

forces opened machine gun fire on men trying to escape the flaming wreckage. Radio operators onboard the American ship finally sent a successful communication to Israeli forces, identifying the *Liberty*.

The barrage ceased, and Israeli forces notified government and intelligence officials, that they had mistakenly fired upon an American vessel. The Israeli government reported the incident immediately to the United States embassy in Tel Aviv, and notified U.S. officials in Washington, D.C. United States Naval Command deployed nearby ships in a belated rescue effort. Before U.S. aid vessels arrived, Israeli and Soviet vessels in the area both offered assistance to the crew of the *Liberty*. McGonagle and his crew refused their aid.

Though the incident was shrouded in secrecy for numerous years, the U.S. government declassified most of the documents surrounding the Israeli attack on the *Liberty* in the mid 1990s. Though some people, including various crewmembers, remain skeptical about the motive and nature of Israeli military actions against the ship, the Liberty Incident was officially ruled a "friendly fire" accident. Volumes of documents and diplomatic evidence materials support this conclusion.

In July 1967, the U.S. Navy conducted the first official investigation of the Liberty Incident. The investigation team collaborated Israeli accounts that the ship was hastily misidentified as result of wartime stresses on military and intelligence resources. The inquiry noted relatively calm seas prevented the ship's flags from visible flight, and that jammed radios onboard the ship hampered communication. Furthermore, the Navy acknowledged that officials did not report the position of the USS *Liberty* to Israeli intelligence. Twelve subsequent, individual investigations, nine by the United States government and three by Israeli officials, concluded that the attack on the *Liberty* was the result of error. Israel officially apologized for the incident on several occasions, and paid $13 million in reparations. Despite the incident, the United States and Israel maintained increasingly good diplomatic relations. On December 17, 1987, the two governments formally closed diplomatic discussions on the incident.

The USS *Liberty* was not the only Liberty-class intelligence vessel involved in an international incident. The *Liberty*'s sister ship, the USS *Pueblo* was seized by North Korean forces while conducting surveillance missions in international waters off the Korean Peninsula.

FURTHER READING:

BOOKS:

Gerhard, William D. *Attack on the USS Liberty.* Laguna Hills, CA: Aegean Park, 1996.

Cristol, A. Jay. *The Liberty Incident: The 1967 Attack on the U.S. Navy Spy Ship.* Washington, D.C.: Brassey's Military, 2002.

SEE ALSO

Israel, Intelligence and Security
Pueblo *Incident*
Radio, Direction Finding Equipment

USSTRATCOM (United States Strategic Command)

United States Strategic Command, or USSTRATCOM, was formed by a 2002 merger between the Air Force Strategic Command and the U.S. Space Command. Located at Offutt Air Force Base in Nebraska, USSTRATCOM is one of nine unified commands in the Department of Defense. It serves as the command and control center for U.S. strategic forces, as well as military space operations, including the operation of military satellites. In its function as a strategic command center, it is responsible both for early warning against missile attack, as well as the launch of missiles in response.

The Strategic Command portion of USSTRATCOM had its beginnings in March 1946, with the establishment of the U.S. Air Force Strategic Air Command (SAC) at Offutt. At the height of the Cold War, Offutt was the command center for the defense "triad": the strategic bombers and ICBMs (intercontinental ballistic missiles) of the Air Force, and the U.S. Navy's submarine-launched ballistic missiles. On June 1, 1992, with the Cold War over, SAC and the Navy's Joint Strategic Target Planning Staff merged as the U.S. Strategic Command. Thenceforth, all planning, targeting, and wartime deployment of strategic forces would be under a single command, while the day-to-day operations remained with the respective services.

The U.S. Space Command had its roots in the military launches that began in the wake of the Soviets' deployment of the *Sputnik* satellite in 1957. The most visible portions of the space program were the Pioneer and Apollo programs, but Army, Navy, and Air Force activities in space continued throughout the 1960s, 1970s, and 1980s. In September 1985, the Joint Chiefs of Staff created the U.S. Space Command to unify these efforts. During the Persian Gulf War and other military engagements of the 1990s, satellites under the Space Command assisted in surveillance, reconnaissance, and targeting.

USSTRATCOM, established on October 1, 2002, is responsible both for early warning and defense against missile attack and long-range conventional attacks. It is also charged with deterring and defending against the proliferation of weapons of mass destruction. Some 2,500 personnel, representing all four services, along with Department of Defense civilians and contractors, work at the command center. Located in the Underground Command Complex at Offutt, a two-level, 14,000-square-foot (1,301 square mile) reinforced concrete and steel structure, the Command Center is housed alongside the Intelligence Operations Center, Weather Support Center, Force Status Readiness Center, and other support offices.

FURTHER READING:

PERIODICALS:

Clinton, William J. "Remarks on Arrival at Offutt Air Force Base in Bellevue, Nebraska." *Weekly Compilation of Presidential Documents* 36, no. 50 (December 18, 2000): 3041.

Garth, Jeff. "Retired General to Oversee Nuclear Weapons Labs." *New York Times.* (June 17, 1999): A15.

Gordon, Michael R. "U.S. Arsenal: Treaties vs. Nontreaties." *New York Times.* (November 14, 2001): A12.

Myers, Steven Lee. "U.S. 'Updates' All-Out Atom War Guidelines." *New York Times.* (December 8, 1997): A3.

ELECTRONIC:

United States Strategic Command. <http://www.stratcom.af.mil/> (March 28, 2003).

SEE ALSO

Ballistic Missiles
DoD (United States Department of Defense)
Nuclear Weapons
Satellites, Spy

V

Vaccination

United States President George W. Bush authorized a program on December 13, 2002, which by its conclusion, will see approximately 500,000 military personnel vaccinated against smallpox, along with an equal number of key healthcare providers in the United States. In the event of a biological attack that would expose Americans to smallpox, the affected citizens could then be quickly vaccinated by the protected healthcare workers. Additionally, the vaccine will be offered to up to ten million police, firefighters, and other first responders to emergencies. Smallpox vaccination within three days of exposure will usually prevent development of the disease, or dramatically reduce its virulence. Plentiful stocks are on hand in the U.S. to respond to a large smallpox outbreak, and vaccine in quantities necessary for inoculation of the entire population of the United States are in production. By mid-2004, health officials plan to have smallpox vaccinations available on a voluntary basis for all Americans.

An anthrax vaccine is also available and is only routinely given to laboratory workers who are involved with *B. anthracis* study or cultures. Vaccination for anthrax prevention involves a series of six injections over an 18-month period. Over 500,000 military personnel received the vaccine as a precaution in 2002, but for the general population, including medical providers and first responders, the vaccine is not currently recommended as other options such as antibiotic treatment offer protection to individuals exposed to anthrax-causing bacteria.

Diseases like anthrax and smallpox are among those microbial diseases that could be exploited as biological weapons. Indeed, anthrax was sent through the postal system to targets in the United States in the aftermath of the September 11, 2001 terrorist attacks in the U.S. Anthrax is a disease caused by the bacterium *Bacillus anthracis*, which can infect the skin, digestive tract, or lungs. Lung infection is often fatal. Smallpox is an extremely contagious disease that is caused by the variola virus.

Vaccination refers to the procedure in which the presence of a component of a microorganism such as a protein (the antigen) stimulates the defense mechanism of the host, which is known as the immune system, to form an antibody. Each antibody is formed in specific response to a particular antigen. The antibodies act to protect the host from future exposure to the antigen (immunity). Depending on the disease and the nature of the vaccine, the immunity can last from a year or two (i.e., influenza) to a lifetime.

Vaccination is protective against infection without the need of suffering through a bout of a disease. In this artificial process an individual receives the antibody-stimulating compound either by injection or orally. Some vaccines like that for smallpox do contain live microorganisms, which can cause some discomfort and, in rare cases, more serious complications. Nonetheless, for most people, vaccination is a prudent step to avoid the threat of a disease. As of early 2003, only one healthcare worker having received the recent smallpox vaccine reported a related complication, a non-life threatening vaccina rash. Less than a dozen instances of complication (none considered serious) have been reported among military personnel receiving the vaccine.

The technique of vaccination has been practiced since at least the early decades of the eighteenth century. Then, a common practice in Istanbul, Turkey was to retrieve material from the surface sores of a smallpox sufferer and rub the material into a cut on another person. The recipient was often spared the ravages of smallpox. This practice was noted by Lady Mary Wortley Montague, the wife of the British Ambassador Extraordinary to the Turkish court. Upon her return to England, she used her social standing to promote the benefits of this crude method of smallpox inoculation. Among those who were convinced was the Royal Family. Indeed, it became fashionable to receive an inoculation, partly perhaps it carried social

cache. The technique was refined by Edward Jenner into a vaccine for cowpox in 1796.

Since Jenner's time, vaccines for a variety of bacterial and viral maladies have been developed. The material used for vaccination is one of four types. Some vaccines consist of living but weakened viruses. Such an attenuated vaccine does not cause an infection but does elicit an immune response. An example is the measles, mumps, and rubella (MMR) vaccine. The second type of vaccine can involve killed viruses or bacteria. The virus or bacteria need to be killed in a way that does not perturb their surfaces. This care is necessary to preserve the three-dimensional structure of surface molecules that stimulate the immune response. Agents such as alum can be used to enhance the immune response to the killed target, perhaps by exposing the antigen to the immune system for a longer time. A third type of vaccination involves a toxoid, which is an inactivated form of a toxin produced by the target bacterium. Examples of toxoid vaccines are the diphtheria and tetanus vaccines. Lastly, a biosynthetic vaccine can utilize a synthetic compound pieced together from portions of two antigens. The Hib vaccine is a biosynthetic vaccine.

Vaccinations against some diseases occurs early in life. For example, during an infant's first two years of life, a series of vaccinations is recommended to develop protection against hepatitis B, polio, measles, mumps, rubella (also called German measles), pertussis (also called whooping cough), diptheriae, tetanus (lockjaw), *Haemophilus influenzae* type b, pneumococcal infections, and chickenpox. Multiple injections of the vaccine can be required to ensure that the immunity that develops is long lasting. For example, vaccination against diphtheria, tetanus, and pertussis is typically administered at 2 months of age, 4 months, 6 months, 15 to 18 months, and finally at 4 to 6 years of age.

A series of vaccinations such as the above triggers a greater production of antibody by the immune system.

The immune cells that respond to the presence of an antigen in a vaccine are called lymphocytes. Prior to vaccination there are a multitude of lymphocytes, each of which recognizes a single specific protein or a portion of the protein. The presence of a specific antigen stimulates that lymphocyte that recognizes the antigenic target. That lymphocyte will then divide repeatedly and the daughter cells will produce antibody. Eventually, there are many daughter lymphocytes and a lot of antibody circulating in the body.

If the antigen does not persist in the body, the production of antibodies will stop. But the lymphocytes that have been produced still retain the memory of the target protein. When the target is presented again to the lymphocytes, as happens in the second vaccination in a series, the many lymphocytes are stimulated to divide into daughter cells, which in turn form antibodies. This is because the immune cells that responded to the antigen upon the first exposure "remember" the antigen, and so can produce even more antibody when presented with the antigen a second or third time. In immunological terms the immune cells are said to be "primed." This form of antigenic memory can last for a lifetime for diseases such as diphtheria and pertussis. For other diseases such as tetanus adults should be vaccinated every ten years (a "booster shot") in order to keep their bodies primed to fight the tetanus microorganism.

Many vaccinations are given via injection. However, solutions that can be drunk are also used. The classic example is the oral vaccine to polio devised by Albert Sabin. Oral vaccination is often limited by the passage of the vaccine through the highly acidic stomach. In the future is hoped that the bundling of the vaccine in a protective casing will prevent the damage caused in the stomach. Experiments using bags made out of lipid molecules (liposomes) has demonstrated both protection of the vaccine and the ability to tailor the liposome release of the vaccine.

While the benefits of vaccination are obvious, this protection against disease does not come without a risk. For a variety of vaccines, side effects are possible. For some vaccines, the side effects are minor. A person may, for example, develop a slight ache and redness at the site of injection. In some very rare cases, however, more severe reactions can occur, such as convulsions and high fever. The smallpox vaccine carries the risk of encephalitis (swelling of cells of the brain and spinal cord) in approximately three to 12 people per million people vaccinated.

FURTHER READING:

BOOKS:

Joellenbeck, Lois M., Lee L. Zwanziger, Jane S. Durch, and Brian L. Strom. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington: Joseph Henry Press, 2002.

Murphy, Christine. *The Vaccine Dilemma.* New York: Lantern Books, 2000.

Neustaedter, Randall. *The Vaccine Guide: Risks and Benefits for Children and Adults.* Berkeley: North Atlantic Books, 2002.

ELECTRONIC:

Centers for Disease Control and Prevention. "Vaccine Fact Sheets." National Vaccine Program Office. November 23, 2002. <http://www.cdc.gov/od/nvpo/fs_toc.htm>(6 January 2003).

SEE ALSO

Biocontainment Laboratories
Biological Warfare
Pathogens

Vaccine Event Reporting System.

SEE *Anthrax Vaccine.*

Vaccines

JULI BERWALD

A vaccine is a medical preparation given to a person to provide immunity from a disease. Vaccines use a variety of different substances ranging from dead microorganisms to genetically engineered antigens to defend the body against potentially harmful antigens. Effective vaccines change the immune system by promoting the development of antibodies that can quickly and effectively attack disease causing microorganisms or viruses when they enter the body, preventing disease development.

Vaccine Development

The development of vaccines against diseases including polio, smallpox, tetanus, and measles is considered among one of the great accomplishments of medical science. Researchers are continually attempting to develop new vaccinations against other diseases. In particular, vigorous research into vaccines for Acquired Immune Deficiency Syndrome (AIDS), cancer and Severe Acute Respiratory Syndrome (SARS) is currently underway.

The first successful vaccine was developed from cowpox as a treatment for smallpox. Coined by Louis Pasteur (1822–1895), the etymology of the term vaccine reflects this achievement. It is taken from the Latin for cow (*vacca*) and the word vaccinia, the virus that causes cowpox.

Smallpox. The first effective vaccine developed treated smallpox, a virulent disease that killed thousands of its victims and left thousands of others disfigured. In one of the first forms of inoculation, the ancient Chinese developed a snuff made from powdered smallpox scabs that was blown into the nostrils of uninfected individuals. Some individuals died from the therapy; however, in most cases, the mild infection produced offered protection from later, more serious infection.

In the late 1600s, European peasants employed a similar method of immunizing themselves against smallpox. In a practice referred to as "buying the smallpox," peasants in Poland, Scotland, and Denmark reportedly injected the smallpox virus under the skin to obtain immunity.

Lady Mary Wortley Montague, the wife of the British ambassador to Turkey brought information on immunization back to Europe in the early 1700s. Montague reported that the Turks injected a preparation of smallpox scabs into the veins of susceptible individuals. Those injected generally developed a mild case of smallpox from which they recovered rapidly. Montague convinced King George I to allow trials of the technique on inmates in Newgate Prison. Although some individuals died after receiving the injections, the trials were successful enough that variolation, or the direct injection of smallpox, became accepted medical practice. Variolation also was credited with protecting United States soldiers from smallpox during the Revolutionary War.

Edward Jenner (1749–1823), an English country physician, observed that people who were in contact with cows often developed cowpox, which caused pox sores but was not life threatening. Those people never developed smallpox. In 1796, Jenner tested the hypothesis that cowpox could be used to protect humans against smallpox. He injected a healthy eight-year-old boy with cowpox obtained from a milkmaid's sore. The boy was moderately ill and recovered. Jenner then injected the boy twice with the smallpox virus, and the boy did not get sick.

Modern knowledge of the immune system suggests that the virus that causes cowpox is similar enough to the virus that causes smallpox that the vaccine simulated an immune response to smallpox. Exposure to cowpox antigen stimulated the boy's immune system, producing cells that attacked the original antigen as well as the smallpox antigen. The vaccine also conditioned the immune system to produce antibodies more quickly and more efficiently against future infection by smallpox.

During the two centuries since its development, the smallpox vaccine gained popularity, protecting millions from contracting the disease. In 1979, following a major cooperative effort between nations and several international organizations, world health authorities declared smallpox the only infectious disease to be eradicated from the planet.

Rabies. In 1885 Louis Pasteur (1822–1895) saved the life of Joseph Meister, a nine year old who had been attacked by a rabid dog. Pasteur's series of experimental rabies vaccinations on the boy proved the effectiveness of the new vaccine.

Pasteur's rabies vaccine, the first human vaccine created in a laboratory, was made of an extract gathered from the spinal cords of rabies-infected rabbits. The live virus was weakened by drying over potash. The new vaccination was far from perfect, causing occasional fatalities and temporary paralysis. Individuals had to be injected 14 to 21 times.

The rabies vaccine has been refined many times. In the 1950s, a vaccine grown in duck embryos replaced the use of live virus, and in 1980, a vaccine developed in cultured human cells was produced. In 1998, the newest vaccine technology—genetically engineered vaccines—was applied to rabies. The new DNA vaccine cost a fraction of the regular vaccine. While only a few people die of rabies each year in the United States, more than 40,000 die worldwide, particularly in Asia and Africa. The less expensive vaccine will make vaccination far more available to people in less developed nations.

Polio. In the early 1900s polio was extremely virulent in the United States. At the peak of the epidemic, in 1952, polio killed 3,000 Americans, and 58,000 new cases of polio were reported.

In 1955 Jonas Salk (1914–1995) developed a vaccine for poliomyelitis. The Salk vaccine, a killed virus type, contained the three types of poliovirus that had been identified in the 1940s. In the first year the vaccine was distributed, dozens of cases of polio were reported in individuals who had received the vaccine or had contact with individuals who had been vaccinated. This resulted from an impure batch of vaccine that had not been completely inactivated. By the end of the incident, more than 200 cases had developed and 11 people had died.

In 1961, an oral polio vaccine developed by Albert B. Sabin (1906–1993) was licensed in the United States. The Sabin vaccine, which uses weakened, live polio viruses, quickly overtook the Salk vaccine in popularity in the United States, and is currently administered to all healthy children. Because it is taken orally, the Sabin vaccine is more convenient and less expensive to administer than the Salk vaccine.

Advocates of the Salk vaccine, which is still used extensively in Canada and many other countries, contend that it is safer than the Sabin oral vaccine. No individuals have developed polio from the Salk vaccine since the 1955 incident. In contrast, the Sabin vaccine has a very small but significant rate of complications, including the development of polio. However, there has not been one new case of polio in the United States since 1975, or in the Western Hemisphere since 1991. Though polio has not been completely eradicated, there were only 144 confirmed cases worldwide in 1999.

Influenza. Developing a vaccine against the influenza virus is problematic because the viruses that cause the flu constantly evolve. Scientists grapple with predicting what particular influenza strain will predominate in a given year. When the prediction is accurate, the vaccine is effective. When they are not, the vaccine is often of little help. However, the flu shot has had enough success that pediatricians are now recommending the vaccine for children older than 6 months.

AIDS Vaccine Research

Since the emergence of AIDS in the early 1980s, research for a treatment for the disease has resulted in clinical trials for more than 25 experimental vaccines. These range from whole-inactivated viruses to genetically engineered types. Some have focused on a therapeutic approach to help infected individuals to fend off further illness by stimulating components of the immune system; others have genetically engineered a protein on the surface of HIV to prompt immune response against the virus; and yet others attempted to protect uninfected individuals. The challenges in developing a protective vaccine include the fact that HIV appears to have multiple viral strains and mutates quickly.

In January 1999, a promising study was reported in *Science* magazine of a new AIDS vaccine created by injecting a healthy cell with DNA from a protein in the AIDS virus that is involved in the infection process. This cell was then injected with genetic material from cells involved in the immune response. Once injected into the individual, this vaccine "catches the AIDS virus in the act," exposing it to the immune system and triggering an immune response. This discovery offers considerable hope for development of an effective vaccine. As of April, 2003, a vaccine for AIDS had not been proven in clinical trials.

Cancer Vaccine Research

Stimulating the immune system is considered key by many researchers seeking a vaccine for cancer. Currently numerous clinical trials for cancer vaccines are in progress, with researchers developing experimental vaccines against cancer of the breast, colon, and lung, among others. Promising studies of vaccines made from the patient's own tumor cells and genetically engineered vaccines have been reported. Other experimental techniques attempt to penetrate the body in ways that could stimulate vigorous immune responses. These include using bacteria or viruses, both known to efficiently circulate through the body, as carriers of vaccine antigens. These bacteria or viruses could be treated or engineered to make them incapable of causing illness.

Vaccine Production

The classic methods for producing vaccines use biological products obtained directly from a virus or a bacteria. Depending on the vaccination, the virus or bacteria is either used in a weakened form, as in the Sabin oral polio vaccine; killed, as in the Salk polio vaccine; or taken apart so that a piece of the microorganism can be used. For example, the vaccine for *Streptococcus pneumoniae*, which causes pneumonia, uses bacterial polysaccharides, carbohydrates found in bacteria which contain large numbers of monosaccharides, a simple sugar. The different methods for producing vaccines vary in safety and efficiency. In general, vaccines that use live bacterial or viral products are extremely effective when they work, but carry a greater risk of causing disease. This is most threatening to individuals whose immune systems are weakened, such as individuals with leukemia. Children with leukemia are advised not to take the oral polio vaccine because they are at greater risk of developing the disease. Vaccines which do not include a live virus or bacteria tend to be safer, but their protection may not be as great.

The classic types of vaccines are all limited in their dependence on biological products, which often must be kept cold, may have a limited life, and can be difficult to produce. The development of recombinant vaccines—those using chromosomal parts (or DNA) from a different

organism—has generated hope for a new generation of man-made vaccines. The hepatitis B vaccine, one of the first recombinant vaccines to be approved for human use, is made using recombinant yeast cells genetically engineered to include the gene coding for the hepatitis B antigen. Because the vaccine contains the antigen, it is capable of stimulating antibody production against hepatitis B without the risk that live hepatitis B vaccine carries by introducing the virus into the blood stream.

DNA vaccines. As medical knowledge has increased—particularly in the field of DNA vaccines—researchers are working towards developing new vaccines for cancer, melanoma, AIDS, influenza, and numerous others. Since 1980, many improved vaccines have been approved, including several genetically engineered (recombinant) types which first developed during an experiment in 1990. These recombinant vaccines involve the use of so-called "naked DNA." Microscopic portions of a virus's DNA are injected into the patient. The patient's own cells then adopt that DNA, which is then duplicated when the cell divides, becoming part of each new cell. Researchers have reported success using this method in laboratory trials against influenza and malaria. These DNA vaccines work from inside the cell, not just from the cell's surface, as other vaccines do, allowing a stronger cell-mediated fight against the disease. Also, because the influenza virus constantly changes its surface proteins, the immune system or vaccines cannot change quickly enough to fight each new strain. However, DNA vaccines work on a core protein, which researchers believe should not be affected by these surface changes.

Vaccination programs. The Children's Vaccine Initiative, supported by the World Health Organization, the United Nations' Children's Fund, and other organizations, are working diligently to make vaccines easier to distribute in developing countries. More than four million people, mostly children, die every year from preventable diseases. Annually, measles kills 1.1 million children worldwide; whooping cough (pertussis) kills 350,000; hepatitis B 800,000; Haemophilus influenzae type b (Hib) 500,000; tetanus 500,000; rubella 300,000; and yellow fever 30,000. Another 8 million die from diseases for which vaccines are still being developed. These include pneumococcal pneumonia (1.2 million); acute respiratory virus infections (400,000), malaria (2 million); AIDS (2.3 million); and rotavirus (800,000). In August 1998, the Food and Drug Administration approved the first vaccine to prevent rotavirus—a severe diarrhea and vomiting infection.

Effective vaccines have limited many of the life-threatening infectious diseases. In the United States, children starting kindergarten are required to be immunized against polio, diphtheria, tetanus, and several other diseases. Other vaccinations are used only by populations at risk, individuals exposed to disease, or when exposure to a disease is likely to occur due to travel to an area where the disease is common. These include influenza, yellow fever, typhoid, cholera, and Hepatitis A and B.

The measles epidemic of 1989 was a graphic display of the failure of many Americans to be properly immunized. A total of 18,000 people were infected, including 41 children who died after developing measles, an infectious, viral illness whose complications include pneumonia and encephalitis. The epidemic was particularly troubling because an effective, safe vaccine against measles has been widely distributed in the United States since the late 1960s. By 1991, the number of new measles cases had started to decrease, but health officials warned that measles remained a threat.

This outbreak reflected the limited reach of vaccination programs. Only 15% of the children between the ages of 16 and 59 months who developed measles between 1989 and 1991 had received the recommended measles vaccination. In many cases parents erroneously reasoned that they could avoid even the minimal risk of vaccine side effects "because all other children were vaccinated."

Nearly all children are immunized properly by the time they start school. However, very young children are far less likely to receive the proper vaccinations. Problems behind the lack of immunization range from the limited health care received by many Americans to the increasing cost of vaccinations. Health experts also contend that keeping up with a vaccine schedule, which requires repeated visits, may be too challenging for Americans who do not have a regular doctor or health provider.

Internationally, the challenge of vaccinating large numbers of people has also proven to be immense. Also, the reluctance of some parents to vaccinate their children due to potential side effects has limited vaccination use. Parents in the United States and several European countries have balked at vaccinating their children with the pertussis vaccine due to the development of neurological complications in a small number of children given the vaccine. Because of incomplete immunization, whooping cough remains common in the United States, with 30,000 cases and about 25 deaths due to complications annually. One response to such concerns has been testing in the United States of a new pertussis vaccine that has fewer side effects.

Vaccines against biological weapons. The United States Centers for Disease Control have identified six diseases that are the most likely to be used in biological weapons. They are smallpox, anthrax, plague, botulism, tularemia and viral hemorrhagic fevers. Vaccines against these diseases are in various stages of development and dissemination.

After smallpox was eradicated from the United States in 1972, vaccination against the disease was discontinued. As a result, there are a substantial number of people in the United States that have never been exposed to the virus. A

majority of those vaccinated may have waning immunity because the smallpox vaccine provides a high level of immunity for approximately five years, with declining immunity thereafter. The United States has recently stockpiled enough vaccine to control an outbreak in case of a crisis, and plans are underway to increase vaccine production until stockpiles include enough vaccine to inoculate the entire U.S. population against smallpox.

Anthrax is of particular note as a biological weapon because it is an airborne pathogen that can be used in conjunction with traditional weapons. A vaccine against anthrax has recently been developed and it consists of a series of six subcutaneous injections. Because antibiotics are effective against the disease, the vaccine is currently only administered to populations at high risk, such as military personnel and researchers who handle the bacterium that causes anthrax.

Tularemia is caused by the bacterium *Francisella tularensis*, which is an extremely infectious airborne pathogen. Tularemia is usually treated with antibiotics, but a vaccine has been developed and the Food and Drug Administration is currently testing it. To date the vaccine has only been administered to laboratory workers who contact the pathogen on a regular basis.

Vaccines against several diseases that are of concern as biological weapons have not yet been developed. Plague is caused by a bacterium *Yersina pestis* that is often carried by rat mites. Although research is ongoing, there is no vaccine against this disease and one is unlikely to be developed for several years. Botulism is caused by a toxin produced by the bacterium *Clostridium botulinum*. Although an antitoxin that reduces the severity of the symptoms is available, there is no vaccine against botulism. Viral hemorrhagic fevers are caused by any one of several viruses including Ebola, Marburg, Lassa and Machupo. No vaccine against these pathogens is currently available.

FURTHER READING:

BOOKS:

Joellenbeck, L. M., L. L. Zwanziger, J. S. Durch, et al. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington, DC: National Academies Press, 2002.

Preston, R. *The Demon in the Freezer.* New York: Random House, 2002.

PERIODICALS:

Bradley, K. A., J. Mogridge, M. Mourey, et al. "Identification of the Cellular Receptor for Anthrax Toxin." *Nature* no. 414 (2001): 225–29.

Friedlander, A. M. "Tackling Anthrax." *Nature* no. 414 (2001): 160–61.

Henderson, D. A. "Smallpox: Clinical and Epidemiologic Features." *Emerging Infectious Diseases* no. 5 (1999): 537–39.

Rosenthal, S. R., M. Merchlinsky, C. Kleppinger, et al. "Developing New Smallpox Vaccines." *Emerging Infectious Diseases* no. 7 (2001): 920–26.

ELECTRONIC:

Centers for Disease Control and Prevention. "Smallpox Factsheet: Vaccine Overview." Public Health Emergency Preparedness and Response. December 9, 2002. <http://www.bt.cdc.gov/agent/smallpox/vaccination/facts.asp>(31 December 2002).

Rhode Island Department of Health: Bioterrorism Preparedness Program "History of Biological Warfare and Current Threat." <http://www.healthri.org/environment/biot/history.htm> (March 12, 2003).

SEE ALSO

Anthrax Vaccine
Biomedical Technologies
Biological Warfare
Pathogen Transmission
Surgeon General and Nuclear, Biological, and Chemical Defense, United States Office
Variola Virus

Variola Virus

JULI BERWALD

Variola virus (or *variola major*) is the virus that causes smallpox. The virus is one of the members of the poxvirus group (*Poxviridae*) and it is one of the most complicated animal viruses. The variola virus is extremely virulent and is among the most dangerous of all the potential biological weapons.

The variola virus particle is shaped like a biconcave brick 200 to 400 nm long. Its inner compartment contains a highly compressed double strand of deoxyribonucleic acid as well as about 100 proteins and 10 viral enzymes. The enzymes are used in nucleic acid replication. Variola DNA contains about 250,000 base pairs, which make up about 200 genes. The depressions in the brick shape contain structures called lateral bodies, whose function is unknown. Two layers of membrane surround the outside of the virus. The outer layer is covered with spikes 20 nm long that are sometimes arranged helically.

The variola virus attaches to membrane receptors on the exterior of the host cell. The exact mechanisms involved in the binding to and penetration of the host membrane are not known. As it enters the cell, however, the virus loses its exterior membrane coat. Once inside the cell the interior membrane layer is removed and the virus's proteins, enzymes and DNA are released into the cytoplasm of the host cell where viral replication and assembly takes place. The first step in replicating the virus DNA involves a particular set of virus enzymes called Type

I topiosomerase enzymes, which uncoil the compressed strands of variola DNA and aid in replicated the *early genes*. The second step of genome replication involves replicating the *late genes*. During the replication of the variola DNA, large concatamers are formed and subsequently cleaved to form individual virus genomes. The variola virus appears to be able to replicate itself without using any of the host cell's replication machinery. Individual viruses are assembled with the help of the Type I topiosomerase enzymes. It is thought that viral membranes are taken from the cisternae between the host's Golgi apparatus and endoplasmic reticulum. As new viruses are released from the host cell, this Golgi derived membrane is traded for the host's cell membrane. Release occurs about 12 hours after initial infection. The production of variola virus by the host cell usually results in host cell death.

Variola virus infects only humans and can be easily transmitted from person to person via the air. Inhalation of only a few virus particles is sufficient to establish an infection. Transmission of the virus is also possible if items such as contaminated linen are handled. The common symptoms of smallpox include chills, high fever, extreme tiredness, headache, backache, vomiting, sore throat with a cough, and sores on mucus membranes and on the skin. As the sores burst and release pus, the afflicted person can experience great pain. Males and females of all ages are equally susceptible to infection. Prior to smallpox eradication approximately one third of patients died—usually within a period of two to three weeks following appearance of symptoms.

The origin of the variola virus in not clear. However, the similarity of the virus and cowpox virus has prompted the suggestion that the variola virus is a mutated version of the cowpox virus. The mutation likely allowed to virus to infect humans. If such a mutation did occur, then it is possible that when early humans became more agricultural and less nomadic, there may have been selective pressure for the cowpox virus to adapt the capability to infect humans.

Vaccination to prevent infection by the variola virus was established in the 1700s. English socialite and public health advocate Lady Mary Wortley Montagu popularized the practice of injection with the pus obtained from smallpox sores as a protection against the disease. This technique became known as variolation. Late in the same century, Edward Jenner successfully prevented the occurrence of smallpox by an injection of pus from cowpox sores. This was the first vaccination. Vaccination against smallpox has been very successful, and the variola virus is the only pathogenic virus that has been eliminated from the natural environment. The last recorded case of smallpox infection was in 1977. Routine vaccination against smallpox was discontinued in the 1980s.

In the late 1990s, a resolution was passed at the World Health Assembly directing that the remaining stocks of variola virus be destroyed to prevent the reemergence of smallpox and the misuse of the variola virus as a biological weapon. At the time only two high-security laboratories were thought to contain variola virus stock: the Centers for Disease Control and Prevention in Atlanta, Georgia, and the Russian State Center for Research on Virology and Biotechnology in Koltsovo, Russia. However, this decision was postponed until 2002, and now the United States government has indicated its unwillingness to comply with the resolution because of security issues related to potential bioterrorism. Destruction of the stocks of variola virus would deprive countries of the material needed to prepare vaccine in the event of the deliberate use of the virus as a biological weapon. This scenario has gained more credence in the past decade, as terrorist groups have demonstrated the resolve to use biological weapons, including smallpox. In addition, intelligence agencies in several Western European countries issued opinions that additional stocks of the variola virus exist in other than the previously authorized locations.

FURTHER READING:

BOOKS:

Hopkins, D. R. *The Greatest Killer: Smallpox in History.* Chicago: University of Chicago Press, 2002.

Preston, R. *The Demon in the Freezer.* New York: Random House, 2002.

PERIODICALS:

Henderson, D. A., T. V. Inglesby, and J. G. Bartlett, et al. "Smallpox as a Biological Weapon: Medical and Public Health Management." *Journal of the American Medical Association* no. 281 (1999): 2127–37.

ELECTRONIC:

Centers for Disease Control and Prevention. "Smallpox." Public Health Emergency Preparedness and Response. November 26, 2002. <http://www.bt.cdc.gov/agent/smallpox/index.asp>(27 November 2002).

SEE ALSO

Biocontainment Laboratories
Biological and Toxin Weapons Convention
Biological Warfare
Biological Warfare, Advanced Diagnostics
Biological Weapons, Genetic Identification
CDC (United States Centers for Disease Control and Prevention)

Venezuela, Intelligence and Security

Since civilian government was restored in 1958, the Venezuelan military and intelligence organizations have

generally operated under the control of a representative democratic government and a succession of democratically elected presidents.

Prior to 1958 Venezuela was governed by a series of *caudillos*or (military or military-controlled governments). Post–World War II transformations in the economy, spurred by the discovery of major oil reserves, resulted in both internal and external pressures to reform Venezuelan government.

Venezuela is a member of OPEC (Organization of Petroleum Exporting Countries), the world's fifth-largest oil producer, and is a major supplier of oil to the United States.

In 2000, social unrest again began to increase in Venezuela and general strikes shut down the oil industry. As of May 2003, confrontations between strikers and government forces have imperiled the continuation in office of chief of state President Hugo Chavez. The military has shown signs of impatience with Chavez's inability to restore order and start an economic recovery. Rumor of coup attempts started to surface in late 2002.

Venezuela continues to be a major exporter of cocaine to the U.S. and local drug-related battles along the border are frequent.

Venezuela's armed forces include the National Armed Forces (*Fuerzas Armadas Nacionales*, Naval Forces (*Fuerzas Navales*), Air Force (*Fuerzas Aereas*), Armed Forces of Cooperation or National Guard (*Fuerzas Armadas de Cooperacion* or *Guardia Nacional*).

Venezuela's intelligence agency is the Intelligence and Preventive Services Directorate (DISIP) but National Guard units have also cooperated with CIA operations.

Because of alleged involvement in the support of drug trafficking, sales of U.S. military hardware, including F-16s, in 1983 was highly controversial. At the time Venezuela was seen as one of the most stable Latin American countries and a U.S. allies against leftist intervention in Central and South America.

FURTHER READING:

BOOKS:

Gilderhus, Mark T. *The Second Century: U.S.-Latin American Relations Since 1889.* Wilmington, DE: Scholarly Resources, 2000.

Hillman, Richard S., John A. Peeler, and Elsa Cardozo da Silva. *Democracy and Human Rights in Latin America.* Westport, CT: Praeger, 2002.

Musicant, Ivan. *The Banana Wars: A History of United States Military Intervention in Latin America from the Spanish-American War to the Invasion of Panama.* New York: Macmillan, 1990.

SEE ALSO

Americas, Modern U.S. Security Policy and Interventions

Venona

ADRIENNE WILMOTH LERNER

The Venona Project was the United States Army's Signal Intelligence Service, and later the National Security Agency, operation to intercept and decrypt high-level Soviet diplomatic communications. The project formally began during World War II, though Soviet communications had been monitored occasionally since World War I. The long-running Venona Project spanned the length of the Cold War, ending in 1980 at the beginning of the period of détente preceding the fall of the Soviet Union. Venona decrypts lead to the arrest of several Soviet NKVD, later KGB, agents operating in the United States, and gave U.S. intelligence information regarding Soviet infiltration of sensitive government departments and classified projects.

Key breakthroughs. The U.S. Army's Signal Intelligence Service formally began the top-secret Venona Project on February 1, 1943. A team of cryptologists established project headquarters in the building of a former girls' school in Arlington, Virginia. The location became known as Arlington Hall. The Venona team began the difficult task of deciphering Soviet diplomatic intercepts gathered by U.S. intelligence since 1939. The collection was unsorted, unanalyzed, and in disarray, but the small Arlington Hall team quickly made key breakthroughs that allowed limited interpretation of the Soviet communications.

After sorting the intercepts by cipher system, origin, and recipient, cryptologists discovered that certain ciphers were used for certain missions. Diplomatic intercepts were different from Soviet intelligence communications, but many of the codes were variations of each other. In all, the initial team identified five separate cryptological systems.

Several key breakthroughs in the Venona Project facilitated the monitoring of Soviet communications by the U.S. intelligence community. Cryptographer Cecil Phillips observed mathematical patterns in one of the Soviet cryptosystems. While the full decoding of these messages remained illusive, the Arlington Hall team was able to identify intercepts from KGB communications. In October 1943, an archaeologist working as a wartime code breaker, Richard Hallock, discovered repetitions and patterns within other Soviet codes. This breakthrough lead to the first partial decoding of Venona intercepts.

Over the next three years, the Arlington Hall team made substantial progress on cracking various Soviet codes. By 1943, most of the intercepts were double-ciphered, utilizing not only the Soviet codes, but also a mathematical encryption system. Without the fortune of recovering a lost Soviet codebook or cipher machine, Arlington Hall code breakers labored to break the complex code system by hand. By the end of World War II, intercepted Soviet communications were being decoded and

BRIDE

~~TOP SECRET~~ [redacted]

EIDER

USSR

Ref. No: S/NBF/T284 (of 23/12/1952)

[redacted] Issued: [redacted]/5/4/1957

Copy No: 205

RE-ISSUE

THE SHADOWING OF "GNAT" (1945)

From: NEW YORK

To: MOSCOW

No: 87 19 Jan. 45

To VIKTOR[i].

[16 groups unrecovered]

ZENZINOV[ii]

[18 groups unrecovered]

DALLIN[iii] and allegedly KERENSKIJ[iv]

[21 groups unrecoverable]

the last three weeks GNAT [KOMAR][v] and DALLIN have been in a great panic. GNAT has noticed that he is being intensively shadowed; moreover he and D.[vi] have received warnings by telephone from some persons or other that CARTHAGE [KARFAGEN][vii] is preparing to hand GNAT over to the HOUSE [DOM][viii]. GNAT is alarmed by the incessant shadowing and is said to be hiring two bodyguards. D. says that he supposes that it is the "GPU"[ix] which is having GNAT shadowed, preparing to do away with him.

The work [OFORMLENIE] on GNAT is being carried out by KANT[x] and JEANNE [ZhANNA][xi]. KANT is acquainted with GNAT personally, but [B% for the most part] gets his information through a neighbour[a].

Distribution

[Continued overleaf]

M.H. file
KOMAR/GNAT

A decoded 1945 message suggesting worry about a soviet defector codenamed "Gnat" (Viktor Andreevich Kravchenko), one of thousands of secret KGB and GRU messages intercepted and decoded by the U.S. Signals Intelligence Unit, which was codenamed VENONA. NSA ARCHIVES.

read with some success, but the process of translating and analyzing the decrypted messages was painstakingly slow.

Venona intelligence. The first successful uses of intelligence information gathered by the Venona Project came in 1945. Though Venona intercepts could only be deciphered in part, and yielded scant information, two events verified their accuracy and uncompromised nature. As Cold War and anti-communist tensions rose in the United States, the FBI investigated the claims of several people who professed to have knowledge of Soviet espionage activities. Agents questioned Whittaker Chambers, who, as early as the 1930s, reported details of suspected Soviet espionage within the U.S. government. His claims had gone unnoticed in the previous decade, but Whittaker provided information on Soviet agents consistent with similar information in Venona intercepts. Later the same year, Elizabeth Bentley, a minor KGB agent and courier, provided FBI agents with a list of Soviet spies operating in the United States, and their codenames. Some of the codenames Bentley provided matched names that frequently appeared in Venona project messages. U.S. intelligence was thus assured that Soviet intelligence had no knowledge of the Venona Project, or the degree to which the security of Soviet diplomatic and intelligence communications had been compromised.

The following year, analyst Meredith Gardner decoded several portions of KGB messages, furthering decryption efforts begun on the cipher system by Cecil Phillips. The Venona team concentrated on decoding intelligence communications between Moscow and a KGB stronghold in New York City. Gardner decoded messages relayed two years earlier in 1944. In the wartime communications, Soviet officials discussed plans for foreign espionage, counterintelligence measures, and high-level secret American projects. Among the secrets passed between the New York KGB Residence and Moscow headquarters were communications regarding U.S. weapons development. Venona intercepts analyzed by Gardner revealed that Soviet intelligence gained top-secret information on the Manhattan Project, the United State's effort to develop the atomic bomb. Arlington Hall provided U.S. intelligence with evidence of an extensive Soviet espionage campaign within the United States. Venona intercepts also yielded information about Soviet intelligence efforts in Latin America and Western Europe.

As Venona intercepts yielded more information about Soviet infiltration of other Allied governments, United States officials shared the intelligence with Britain and France. In 1948, British cryptologists joined the Venona team. The Venona project monitored Soviet communications in the United States and Britain, ferreting out undercover Soviet intelligence agents in both governments. United States Venona intelligence was sent to the FBI and CIA, while MI-5 and MI-6 processed information from the British team.

Breaking the Soviet espionage network in the United States. Information from Venona intercepts led to the arrest of several Soviet spies in the United States. Since Venona documents were not analyzed as they were received, however, most of those identified foreign agents had given secrets to the Soviets during World War II. Though the Soviet Union was a military ally of the United States during the war, sharing secret information remained illegal. Immediately following the war, relations between the two counties deteriorated. Thus most of the Venona intercepts were translated and analyzed in the light of Cold War tensions.

Among the Soviet agents first identified by Venona communications were State Department officers Alger Hiss and Laurence Duggan who gave the Soviets wartime intelligence. Lauchlin Currie, a friend and aide to President Franklin D. Roosevelt, notified Soviet intelligence when agents operating in the United States were dubbed suspicious by U.S. intelligence and law enforcement. Duncan Lee, an assistant to OSS Chief William Donovan, divulged a plethora of intelligence secrets to Moscow. Three members of the Treasury Department sold the Soviets weapons designs, economic assessments, and other classified information. An NSA linguist, William Weisband, who briefly contributed to Venona by translating intercepts, notified Soviet intelligence of the project's existence.

After this early wave of arrests in the 1950s, several more agents were discovered and taken into custody in the following decades. However, the most notorious, and perhaps the most threatening to national security, of the agents identified by Venona intercepts was the network of Soviet atomic spies. Venona intercepts proved that Soviet agents had infiltrated most areas of the Manhattan Project, and had obtained secrets from ultra-secure sites such as the Oak Ridge and Los Alamos. In 1947, Gardner discovered that the Soviets had placed several intelligence sources in the War Department. While Gardner uncovered several dozen codenames in communications regarding atomic secrets, Venona intercepts added to the cases against spies Klaus Fuchs, Theodore Hall, and Julius Rosenberg.

The team first cracked Rosenberg's codenames, Liberal and Antenna, because of a carelessly coded intercept that used both of his cryptonym and also discussed his wife, Ethel, using her real name. The trial of Julius and Ethel Rosenberg drew a mixed public reaction. Federal prosecutors relied on other evidence, most of which was not as compelling, to convict most Soviet informants rather than expose Venona to the public. Historians and journalists who later investigated anomalies in the Rosenberg case similarly did not have access to Venona documents. Several cases, including that of the Rosenbergs, remained contentious within the general public until Venona documents began to be declassified in the mid-1990s.

Venona intercepts not only provided American and British intelligence with the identities of Soviet spies, they also provided information regarding Soviet intelligence

tradecraft. Through Venona communications, the U.S. intelligence community learned how the Soviet network functioned. Venona documents illustrate how agents were recruited. The messages detailed the use of dead letter drops and the process for arranging meetings between agents. Venona intercepts provided information on Soviet counterintelligence operations and efforts to locate defectors in the United States.

The legacy of Venona. During the course of the Venona Project, nearly 2,200 messages were intercepted, decoded, and translated. Though the project officially spanned decades, its greatest successes were in the first decade of the Cold War. The Arlington Hall team decoded most KGB messages intercepted between 1947 and 1952. Soviet diplomatic messages, which used a less complicated cipher and encryption system, were routinely broken until the Soviets changed the cipher in 1957. Messages were often reworked by intelligence personnel, especially when trying to crack recurring codenames.

While the Venona Project was largely a success for the United States, it did have limitations. Messages were difficult to decipher, and the project did not decode messages in real time. In the earliest years of the project, code breakers worked on intercepts that were two and three years old. The process was accelerated in 1953 when Venona code breakers received from U.S. military intelligence the remains of a partially charred Soviet codebook. The book aided cryptographers in breaking the overlaying encryption system of several codes.

The Venona project was so secretive that intelligence officials did not brief President Harry Truman on its existence for several years. Regardless of its secrecy in the United States, Soviet intelligence learned of the operation and conducted counterintelligence against the Venona Project. KGB defectors, agents who fled the Soviet Union for the United States and cooperated with U.S. officials, told U.S. intelligence that KGB headquarters had limited knowledge of the communications surveillance program. Soviet officials placed their confidence in their encryption systems and did not order an immediate change of codes to protect communications security. Soviet double agent and master spy Kim Philby visited Arlington Hall for briefings while stationed in Washington, D.C. between 1949 and 1951. Whether Philby provided KGB headquarters with a detailed report of Venona operations remains unknown, but again, the Soviets did not quickly change their cipher systems.

One of the most contentious assertions of Venona intelligence is the involvement of American political organizations, especially the American Communist Party, in Soviet-led espionage against U.S. interests. Venona intelligence was used to seek out Soviet agents of espionage, but some charge that the project conducted surveillance on citizens and contributed to McCarthy era anti-communist hysteria among government officials. Recently declassified Venona documents show real links between a few radical socialist and communist organizations in the United States, and Soviet espionage during the 1940s through 1960s. However, the majority of American socialist and communist organizations were never mentioned in Venona messages and bore no connection to Soviet espionage efforts.

In 1995, the National Security Agency officially acknowledged the existence of the Venona Project and began the process of declassifying related documents. The declassified materials include project plans and specifications, case files, and copies of the decoded Soviet intercepts.

FURTHER READING:

BOOKS:

Haynes, John E., and Harvey Klehr. *VENONA: Decoding Soviet Espionage in America.* New Haven, CT: Yale University Press, 1999.

PERIODICALS:

Hatch, David A. "VENONA: An Overview." *American Intelligence Journal* 17, no. 1/2 (1996): 71–77.

ELECTRONIC:

United States National Security Agency. *VENONA Project Declassified Documents.* <http://www.nsa.gov/docs/Venona> 2003.

SEE ALSO

Cold War (1945–1950), The Start of the Atomic Age
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Cryptonym
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
NSA (United States National Security Agency)

Vietnam War

JUDSON KNIGHT

The Vietnam War was a struggle between communist and pro-western forces that lasted from the end of World War II until 1975. The communist Viet Minh, or League for the Independence of Vietnam, sought to gain control of the entire nation from its stronghold in the north. Opposing it were, first, France, and later the United States and United Nations forces, who supported the non-communist forces in southern Vietnam. In 1975, in violation of a 1973 peace treaty negotiated to end United States military involvement in South Vietnam and active war against North Vietnam, North Vietnamese forces and South Vietnamese communist sympathizers seized control of South Vietnam

Converted T-28 trainer aircraft and 250-pound bombs used by Meo pilots of Vang Pao's "mini-Air Force," a CIA-sponsored unit that fought against the North Vietnamese in northern Laos in 1972. ©BETTMANN/CORBIS.

and reunited the two countries into a single communist country.

American involvement in Vietnam has long been a subject of controversy. The fighting depended, to a greater extent than in any conflict before, on the work of intelligence forces. Most notable among these were various U.S. military intelligence organizations, as well as the Central Intelligence Agency (CIA).

Early stages. Led by Ho Chi Minh (1890–1969), the Viet Minh aligned themselves with the Soviets from the 1920s. However, they configured their struggle not in traditional communist terms as a class struggle, but as a war for national independence and unity, and against foreign domination. Vietnam at the time was under French control as part of Indochina, and World War II provided the first opportunity for a Viet Minh uprising against the French, in 1940. France, by then aligned with the Axis under the Vichy government, rapidly suppressed the revolt. Nor did the free French, led by General Charles de Gaulle, welcome the idea of Vietnamese independence.

After the war was over, de Gaulle sent troops to resume control, and fighting broke out between French and Viet Minh forces on December 19, 1946. On May 7, 1954, the French garrison at Dien Bien Phu fell to the Viet Minh after an eight-week siege. Two months later, in July 1954, the French signed the Geneva Accords, by which they formally withdrew from Vietnam.

The Geneva Accords divided the country along the 17th parallel, but this division was to be only temporary, pending elections in 1956. However, in 1955 Ngo Dinh Diem declared the southern portion of the nation the Republic of Vietnam, with a capital at Saigon. In 1956, Diem, with the backing of the United States, refused to allow elections, and fighting resumed. The conflict was now between South Vietnam and the communist republic of North Vietnam, whose capital was Hanoi. Fighting the Army of the Republic of Vietnam (ARVN) were not only the regular army forces of the North Vietnamese Army (NVA), but also Viet Cong, guerrillas from the South who had received training and arms from the North.

American involvement. President Dwight D. Eisenhower had already sent the first U.S. military and civilian advisers to Vietnam in 1955, and four years later, two military advisers became the first American casualties in the conflict. The administration of President John F. Kennedy greatly expanded U.S. commitments to Vietnam, such that by late 1962 the number of military advisers had grown to 11,000. At the same time, Washington's support for the unpopular

Former South Vietnamese commando Tran Quoc Hung, left, with fellow commando Pham Ngoc Khanh were recruited by the CIA as intelligence gatherers during the 1960s and 1970s. Both sought recognition for Vietnamese commandos who aided the CIA and the Deaprtment of Defense during the Vietnam conflict. AP/WIDE WORLD PHOTOS.

Diem had faded, and when American intelligence learned of plans for a coup by his generals, the United States did nothing to stop it. Diem was assassinated on November 1, 1963.

Under President Lyndon B. Johnson, U.S. participation in the Vietnam War reached its zenith. The beginnings of the full-scale commitment came after August 2, 1964, when North Vietnamese gunboats in the Gulf of Tonkin attacked the U.S. destroyer *Maddox.* Requesting power from Congress to strike back, Johnson received it in the form of the Gulf of Tonkin Resolution, which granted the president virtual carte blanche to prosecute the war in Vietnam.

High point of the war. As a result of his strengthened position to wage war, and still enjoying broad support from the American public, Johnson launched a bombing campaign against North Vietnam in late 1964, and again in March 1965, after a Viet Cong attack on a U.S. installation at Pleiku. By June 1965, as the first U.S. ground troops arrived, U.S. troop strength stood at 50,000. By year's end, it would be near 200,000.

General William C. Westmoreland, who had assumed command of U.S. forces in Vietnam in June 1964, maintained that victory required a sufficient commitment of ground troops. Yet by the mid-1960s, the NVA had begun moving into the South via the Ho Chi Minh Trail, and as communist forces began to take more villages and hamlets, they seemed poised for victory. Johnson pledged greater support, but despite growing number of ground troops and intensive bombing of the North in 1967, U.S. victory remained elusive.

The turning point in the U.S. effort came on January 30, 1968, when the NVA and Viet Cong launched a surprise attack during celebrations of the Vietnamese lunar new year, or Tet. The Tet Offensive, though its value as a military victory for the North is questionable, was an

enormous psychological victory that convinced Americans that short of annihilation of North Vietnam—an unacceptable geopolitical alternative—they could not win a Korea-like standoff or outright victory in Vietnam. In March 1968, Johnson called for an end to bombing north of the 20th parallel, and announced that he would not seek reelection. Westmoreland, too, was relieved of duty.

Withdrawal (1969–75). The administration of President Richard Nixon in 1969 began withdrawing, and instituted a process of "Vietnamization," or turning control of the war over to the South Vietnamese. In 1970, the most significant military activity took place in Cambodia and Laos, where U.S. B-52 bombers continually pounded the Ho Chi Minh Trail in an effort to cut off supply lines.

Despite the bombing campaign, undertaken in pursuit of Vietnamization and the goal of making the war winnable for the South, the North continued to advance. On January 27, 1973, the United States and North Vietnam signed the Paris Peace Accords, and U.S. military involvement in Vietnam ended.

During the two years that followed, the North Vietnamese gradually advanced on the South. On April 30, 1975, communist forces took control of Saigon as government members and supporters fled. On July 2, 1976, the country was formally united as the Socialist Republic of Vietnam, and Saigon renamed Ho Chi Minh City.

The intelligence and special operations war. Behind and alongside the military war was an intelligence and special operations war that likewise dated back to World War II. At that time, the United States, through the Organization of Strategic Services (OSS), actually worked closely with Viet Minh operatives, who OSS agents regarded as reliable allies against the Japanese. Friendly relations with the Americans continued after the Japanese surrender, when OSS supported the cause of Vietnamese independence.

This stance infuriated the French, who sought to reestablish control while avoiding common cause with the Viet Minh. They attempted to cultivate or create a number of local groups, among them a Vietnamese mafia-style organization, that would work on their behalf against the Viet Minh. These efforts, not to mention the participation of one of the world's most well-trained special warfare contingents, the Foreign Legion, availed the French little gain.

Special Forces, military intelligence, and CIA. In the first major U.S. commitment to Vietnam, Kennedy brought to bear several powerful weapons that together signified his awareness that Vietnam was not a war like the others America had fought: the newly created Special Forces group, known popularly as the "Green Berets," as well as CIA and a host of military intelligence organizations.

Though Special Forces are known popularly for their prowess in physical combat, their mission in Vietnam from the beginning had a strong psychological warfare component. In May 1961, Kennedy committed 400 of these elite troops to the war in Southeast Asia, and more would follow.

Alongside them, in many cases, were military intelligence personnel, whose ranks in Vietnam numbered 3,000 by 1967. Most of these were in two army units, the Army Security Agency (ASA) and the Military Intelligence Corps. The work of military intelligence ranged from the signals intelligence of ASA, one of whose members became the first regular-army U.S. soldier to die in combat in 1961, to the electronic intelligence conducted by navy destroyers such as the ill-fated *Maddox.* In addition, military aircraft such as the SR-71 Blackbird and U-2 conducted extensive aerial reconnaissance.

As for CIA, by the time the war reached its height in the mid- to late 1960s, it had some 700 personnel in Vietnam. Many of these operated undercover groups that included the Office of the Special Assistant to the Ambassador (OSA, led by future CIA chief William Colby), which occupied a large portion of the U.S. Embassy in Saigon.

Cooperation and conflict. These three major arms of the intelligence and special operations war—Special Forces and other elite units, military intelligence, and CIA—often worked together. When Kennedy sent in the first contingent of Special Forces, they went to work alongside CIA, to whom the president in 1962 gave responsibility for paramilitary operations in Vietnam.

Unbeknownst to most Americans, CIA was also in charge of paramilitary operations in two countries where the United States was not officially engaged: Cambodia and Laos. Long before Nixon's campaign to cut off the Ho Chi Minh Trail with strategic bombers, CIA operatives were training a clandestine army of tribesmen and mercenaries in Laos. Ordinary U.S. troops were not involved in this sideshow war in the interior of Southeast Asia: only Special Forces, who—in order to conceal their identity as American troops—bore neither U.S. markings nor U.S. weaponry.

CIA and army intelligence personnel worked on another notorious operation, Phoenix, an attempt to seek out and neutralize communist personnel in South Vietnam during the period from 1967 to 1971. CIA claimed to have killed, captured, or turned as many as 60,000 enemy agents and guerrillas in Phoenix, a project noted for the ruthlessness with which it was carried out. In this undertaking, CIA and the army had the nominal assistance of South Vietnamese intelligence, but due to an abiding U.S. mistrust of their putative allies, the Americans gave the Saigon little actual role in Phoenix.

The military and CIA debacles. In other situations, CIA and military groups did not so much intentionally collaborate as they found themselves thrown together, often at cross-purposes, or at least in ways that were not mutually

beneficial. While U.S. Navy destroyers in the Gulf of Tonkin were monitoring North Vietnamese electronic transmissions, CIA was busy striking at Viet Minh naval facilities with fast craft whose South Vietnamese (or otherwise non-American) crews made CIA involvement deniable. But North Vietnamese intelligence was as capable as its military, and they fired on the *Maddox* in direct response to this CIA operation.

The U.S. military became involved in another CIA debacle when, in 1968, army intelligence tried to resume a failed effort by CIA's Studies and Observation Group (SOG), another cover organization. From the early 1960s, SOG had been attempting to parachute South Vietnamese agents into North Vietnam, with the intention of using them as saboteurs and agents provocateur. The effort backfired, with most of the infiltrators dead, imprisoned, or used by the North Vietnamese as bait. CIA put a stop to the undertaking, but army intelligence tried to succeed where CIA had failed—only to lose several hundred more Vietnamese agents.

The U.S. Air Force had to take over another unsuccessful CIA operation, Black Shield, which involved a series of reconnaissance flights by A-12 Oxcart spy planes over North Vietnam in 1967 and 1968. Using the A-12, which could reach speeds of Mach 3.1 (2,300 m.p.h. or 3,700 k.p.h.), Black Shield gathered extensive information on Soviet-built surface-to-air missile (SAM) installations in the North. To obtain the best possible photographic intelligence, the Oxcarts had to fly relatively low and slow, and in the fall of 1967 North Vietnamese SAMs hit—but did not down—an A-71. In 1968, the U.S. Air Force, operating SR-71 Blackbirds, replaced CIA.

Assessing CIA in Vietnam. Despite the notorious nature of Phoenix or the CIA undertakings in Cambodia and Laos, as well as the occasions when CIA overplayed its hand or placed the military in the position of cleaning up one of its failed operations, CIA involvement in Vietnam was far from an unbroken record of failure. One success was Air America. The latter, a proprietary airline chartered in 1949, supplied the secret war in the interior, and also undertook a number of other operations in Vietnam and other countries in Asia. That Air America was only disbanded in 1981, long after the war ended, illustrates its effectiveness.

The popular image of CIA operatives in Vietnam as fiends blinded by hatred of communism—an image bolstered by Hollywood—is as lacking in historical accuracy as it is in depth of characterization. Like other Americans involved in Vietnam, members of CIA began with the belief that they could and would save a vulnerable nation from Soviet-style totalitarianism and provide its people with an opportunity to develop democratic institutions, establish prosperity, and find peace. Much more quickly than their counterparts in the military and political communities, however, members of the intelligence community came to recognize the fallacies on which their undertaking was based.

Intelligence vs. the military and the politicians. Whereas many political and military leaders adhered to standard interpretations about the North Vietnamese, such as the idea that they were puppets of Moscow whose power depended entirely on force, CIA operatives with closer contact to actual Vietnamese sources recognized the appeal of the Viet Minh nationalist message. And because CIA recognized the strength of the enemy, their estimate of America's ability to win the war—particularly as the troop buildup began in the mid-1960s—became less and less optimistic.

CIA appraisal of the situation tended to be far less sanguine than that of General Westmoreland and other military leaders, and certainly less so than that of President Johnson and other political leaders far removed from the conflict. In 1965, for instance, CIA and the Defense Intelligence Agency (DIA) produced a joint study in which they predicted that the bombing campaign would do little to soften North Vietnam. This was not a position favored by Washington, however, so it received little attention.

Whereas Washington favored an air campaign, General Westmoreland maintained that the war would be won by ground forces. Both government and military leaders agreed on one approach: the use of statistics as a benchmark of success or failure. In terms of the number of bombs dropped, cities hit, or Viet Cong and NVA killed, American forces seemed to be winning. Yet for every guerrilla killed, the enemy seemed to produce two or three more in his place, and every village bombed seemed only to increase enemy resistance.

The lessons of Vietnam. In the end, the United States effort in Vietnam was undone by the singularity of aims possessed by its enemies in the North; the instability and unreliability of its allies in the South, combined with American refusal to give the South Vietnamese a greater role in their own war; and a divergence of aims on the part of American leaders.

For example, the Tet Offensive, which resulted in so many Viet Cong deaths that the guerrilla force was essentially eliminated, and NVA regulars took the place of the Viet Cong, is remembered as a *victory* for the North. And it was a victory in psychological, if not military, terms. The surprise, fear, and disappointment elicited by the Tet Offensive—combined with a rise of political dissent within the United States—punctured America's will to wage the war, and marked the beginning of the end of American participation in Vietnam.

For some time, U.S. college campuses had seen small protests against the war, but in 1968 the number of these demonstrations grew dramatically, as did the ranks of participants. Nor were youth the only Americans now opposing the war in large numbers: increasingly, other sectors of society—including influential figures in the media, politics, the arts, and even the sciences—began to make their opposition known. In the final years of Vietnam, there was a secondary war being fought in the

United States—a war concerning America's vision of itself and its role in the world.

By war's end, Vietnam itself had largely been forgotten. Despite earlier promises of a liberal democratic government, the unified socialist republic fell prey to the exigencies typical of communist dictatorship: mass imprisonments and executions, forced redistribution of land, and the banning of political opposition. Forgotten, too, were Laos and even Cambodia, where the Khmer Rouge launched a campaign of genocide that killed an estimated two million people.

The Vietnamese invasion in 1979 probably saved thousands of Cambodian lives, but in the aftermath, Vietnam came to be regarded as a colonialist power. The nation once admired by the third world for standing up to America now became a pariah, supported only by Moscow—which had gained access to a valuable warm-water port at Cam Ranh Bay—and its allies in Eastern Europe.

During the remainder of the 1970s, America was in retreat, its attention turned away from the fate of countries that fell to communism or, in the case of Iran, to Islamic fundamentalist dictatorship. Americans focused their anger on those they regarded as having led them astray during the war years: politicians, the military, and CIA, which came under intense scrutiny during the 1975–76 Church committee hearings in the U.S. Senate. Only in the 1980s, under President Ronald Reagan, did the United States return to an activist stance globally.

FURTHER READING:

BOOKS:

Allen, George W. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam.* Chicago: Ivan R. Dee, 2001.

Conboy, Kenneth K., and Dale Andradé. *Spies and Commandos: How America Lost the Secret War in North Vietnam.* Lawrence, KS: University Press of Kansas, 2000.

Kissinger, Henry. *Years of Renewal.* New York: Simon and Schuster, 1999.

Shultz, Richard G. *The Secret War against Hanoi: Kennedy's and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam.* New York: HarperCollins, 1999.

Sorley, Lewis. *A Better War: The Unexamined Victories and Final Tragedy of America's Last Years in Vietnam.* New York: Harcourt Brace, 1999.

Wirtz, James J. *The Tet Offensive: Intelligence Failure in War.* Ithaca, NY: Cornell University Press, 1991.

ELECTRONIC:

Vietnam War Declassification Project. Gerald R. Ford Library and Museum. <http://www.ford.utexas.edu/library/exhibits/vietnam/> (February 5, 2003).

SEE ALSO

CIA (United States Central Intelligence Agency)
Cold War (1950–1972)
Cold War (1972–1989): The Collapse of the Soviet Union
Johnson Administration (1963–1969), United States National Security Policy
Kennedy Administration (1961–1963), United States National Security Policy
Nixon Administration (1969–1974), United States National Security Policy

Viral Biology

BRIAN D. HOYLE/ABDEL HAKIM NASR

An understanding of the fundamentals of virus structure, genetics, and replication is critical to virologists and other forensic investigators attempting to identify potential biogenic pathogens that may be exploited as agents in biological warfare or by bioterrorists.

Fundamentals of Viral Biology

Viruses are essentially nonliving repositories of nucleic acid that require the presence of a living prokaryotic or eukaryotic cell for the replication of the nucleic acid. There are a number of different viruses that challenge the human immune system and that may produce disease in humans. In general, a virus is a small, infectious agent that consists of a core of genetic material (either deoxyribonucleic acid [DNA] or ribonucleic acid [RNA]) surrounded by a shell of protein. All viruses share the need for a host in order to replicate their deoxyribonucleic acid (DNA) or ribonucleic acid (RNA). The virus commandeers the host's existing molecules for the nucleic acid replication process. There are a number of different viruses. The differences include the disease symptoms they cause, their antigenic composition, type of nucleic acid residing in the virus particle, the way the nucleic acid is arranged, the shape of the virus, and the fate of the replicated DNA. These differences are used to classify the viruses and have often been the basis on which the various types of viruses were named.

Virology, viral classification, types of viruses. Virology is the discipline of microbiology that is concerned with the study of viruses. Viruses can exist in a variety of hosts. Viruses can infect animals (including humans), plants, fungi, birds, aquatic organisms, protozoa, bacteria, and insects. Some viruses are able to infect several of these hosts, while other viruses are exclusive to one host.

The classification of viruses operates by use of the same structure that governs the classification of bacteria. The International Committee on Taxonomy of Viruses established the viral classification scheme in 1966. From the broadest to the narrowest level of classification, the viral scheme is: Order, Family, Subfamily, Genus, Species,

A man leaves his house while it is fumigated for mosquitos in Costa Rica in an effort to stop a 2002 outbreak of Dengue fever, whose viral hemorrhagic variety can be fatal if not immediately treated. AP/WIDE WORLD PHOTOS.

and Strain/type. To use an example, the virus that was responsible for an outbreak of Ebola hemorrhagic fever in a region of Africa called Kikwit is classified as Order Mononegavirales, Family Filoviridae, Genus *Filovirus*, and Species Ebola virus Zaire.

In the viral classification scheme, all families end in the suffix *viridae*, for example Picornaviridae. Genera have the suffix *virus*. For example, in the family Picornaviridae there are five genera: enterovirus, cardiovirus, rhinovirus, apthovirus, and hepatovirus. The names of the genera typically derive from the preferred location of the virus in the body (for those viral genera that infect humans). As examples, rhinovirus is localized in the nasal and throat passages, and hepatovirus is localized in the liver. Finally, within each genera there can be several species.

There are a number of criteria by which members of one grouping of viruses can be distinguished from those in another group. For the purposes of classification, however, three criteria are paramount. These criteria are the host organism or organisms that the virus utilizes, the shape of the virus particle, and the type and arrangement of the viral nucleic acid.

An important means of classifying viruses concerns the type and arrangement of nucleic acid in the virus particle. Some viruses have two strands of DNA, analogous to the double helix of DNA that is present in prokaryotes such as bacteria and in eukaryotic cells. Some viruses, such as the Adenoviruses, replicate in the nucleus of the host using the replication machinery of the host. Other viruses, such as the Poxviruses, do not integrate in the host genome, but replicate in the cytoplasm of the host. Another example of a double-stranded DNA virus are the Herpesviruses.

Other viruses only have a single strand of DNA. An example is the Parvoviruses. Viruses such as the Parvoviruses replicate their DNA in the host's nucleus. The replication involves the formation of what is termed a negative-sense strand of DNA, which is a blueprint for the subsequent formation of the RNA and DNA used to manufacture the new virus particles.

The genome of other viruses, such as Reoviruses and Birnaviruses, is comprised of double-stranded RNA. Portions of the RNA function independently in the production of a number of so-called messenger RNAs, each of which produces a protein that is used in the production of new viruses.

Still other viruses contain a single strand of RNA. In some of the single-stranded RNA viruses, such as Picornaviruses, Togaviruses, and the Hepatitis A virus, the

RNA is read in a direction that is termed "+ sense." The sense strand is used to make the protein products that form the new virus particles. Other single-stranded RNA viruses contain what is termed a negative-sense strand. Examples are the Orthomyxoviruses and the Rhabdoviruses. The negative strand is the blueprint for the formation of the messenger RNAs that are required for production of the various viral proteins.

Still another group of viruses have + sense RNA that is used to make a DNA intermediate. The intermediate is used to manufacture the RNA that is eventually packaged into the new virus particles. The main example is the Retroviruses (e.g. the Human Immunodeficiency viruses). Finally, a group of viruses consist of double-stranded DNA that is used to produce a RNA intermediate. An example is the Hepadnaviruses.

An aspect of virology is the identification of viruses. Often, the diagnosis of a viral illness relies, at least initially, on the visual detection of the virus. For this analysis, samples are prepared for electron microscopy using a technique called negative staining, which highlights surface detail of the virus particles. For this analysis, the shape of the virus is an important feature.

A particular virus will have a particular shape. For example, viruses that specifically infect bacteria, the so-called bacteriophages, look similar to the Apollo lunar lander (LEM spacecraft). A head region containing the nucleic acid is supported on a number of spider-like legs. Upon encountering a suitable bacterial surface, the virus acts like a syringe, to introduce the nucleic acid into the cytoplasm of the bacterium.

Other viruses have different shapes. These include spheres, ovals, worm-like forms, and even irregular (pleomorphic) arrangements. Some viruses, such as the influenza virus, have projections sticking out from the surface of the virus. These are crucial to the infectious process.

As new species of eukaryotic and prokaryotic organisms are discovered, no doubt the list of viral species will continue to grow.

Viral genetics. Viral genetics, the study of the genetic mechanisms that operate during the life cycle of viruses, utilizes biophysical, biological, and genetic analyses to study the viral genome and its variation.

The virus genome consists of only one type of nucleic acid, which could be a single or double stranded DNA or RNA. Single stranded RNA viruses could contain positive-sense (+RNA), which serves directly as mRNA or negative-sense RNA (–RNA) that must use an RNA polymerase to synthesize a complementary positive strand to serve as mRNA. Viruses are obligate parasites that are completely dependant on the host cell for the replication and transcription of their genomes as well as the translation of the mRNA transcripts into proteins. Viral proteins usually have a structural function, making up a shell around the genome, but may contain some enzymes that are necessary for the virus replication and life cycle in the host cell. Both bacterial virus (bacteriophages) and animal viruses play an important role as tools in molecular and cellular biology research.

Viruses are classified in two families depending on whether they have RNA or DNA genomes and whether these genomes are double or single stranded. Further subdivision into types takes into account whether the genome consists of a single RNA molecule or many molecules as in the case of segmented viruses. Four types of bacteriophages are widely used in biochemical and genetic research. These are the T phages, the temperate phages typified by bacteriophage lambda , the small DNA phages like M13, and the RNA phages. Animal viruses are subdivided in many classes and types. Class I viruses contain a single molecule of double stranded DNA and are exemplified by adenovirus, simian virus 40 (SV40), herpes viruses and human papillomaviruses. Class II viruses are also called parvoviruses and are made of single stranded DNA that is copied in to double stranded DNA before transcription in the host cell. Class III viruses are double stranded RNA viruses that have segmented genomes which means that they contain 10–12 separate double stranded RNA molecules. The negative strands serve as template for mRNA synthesis. Class IV viruses, typified by poliovirus, have single plus strand genomic RNA that serves as the mRNA. Class V viruses contain a single negative strand RNA which serves as the template for the production of mRNA by specific virus enzymes. Class VI viruses are also known as retroviruses and contain double stranded RNA genome. These viruses have an enzyme called reverse transcriptase that can both copy minus strand DNA from genomic RNA catalyze the synthesis of a complementary plus DNA strand. The resulting double stranded DNA is integrated in the host chromosome and is transcribed by the host own machinery. The resulting transcripts are either used to synthesize proteins or produce new viral particles. These new viruses are released by budding, usually without killing the host cell. Both HIV and HTLV viruses belong to this class of viruses.

Virus genetics is studied by either investigating genome mutations or exchange of genetic material during the life cycle of the virus. The frequency and types of genetic variations in the virus are influenced by the nature of the viral genome and its structure. Especially important are the type of the nucleic acid that influence the potential for the viral genome to integrate in the host, and the segmentation that influence exchange of genetic information through assortment and recombination.

Mutations in the virus genome could either occur spontaneously or be induced by physical and chemical means. Spontaneous mutations that arise naturally as a result of viral replication are either due to a defect in the genome replication machinery or to the incorporation of

an analogous base instead of the normal one. Induced virus mutants are obtained by either using chemical mutants like nitrous oxide that acts directly on bases and modify them or by incorporating already modified bases in the virus genome by adding these bases as substrates during virus replication. Physical agents such as ultraviolet light and x rays can also be used in inducing mutations. Genotypically, the induced mutations are usually point mutations, deletions, and rarely insertions. The phenotype of the induced mutants is usually varied. Some mutants are conditional lethal mutants. These could differ from the wild type virus by being sensitive to high or low temperature. A low temperature mutant would for example grow at 31°C but not at 38°, while the wild type will grow at both temperatures. A mutant could also be obtained that grows better at elevated temperatures than the wild type virus. These mutants are called hot mutants and may be more dangerous for the host because fever, which usually slows the growth of wild type virus, is ineffective in controlling them. Other mutants that are usually generated are those that show drug resistance, enzyme deficiency or an altered pathogenicity or host range. Some of these mutants cause milder symptoms compared to the parental virulent virus and usually have potential in vaccine development as exemplified by some types of influenza vaccines.

Besides mutation, new genetic variants of viruses also arise through exchange of genetic material by recombination and reassortment. Classical recombination involves breaking of covalent bonds within the virus nucleic acid and exchange of some DNA segments followed by rejoining of the DNA break. This type of recombination is almost exclusively reserved to DNA viruses and retroviruses. RNA viruses that do not have a DNA phase rarely use this mechanism. Recombination usually enables a virus to pick up genetic material from similar viruses and even from unrelated viruses and the eukaryotic host cells. Exchange of genetic material with the host is especially common with retroviruses. Reassortment is a non-classical kind of recombination that occurs if two variants of a segmented virus infect the same cell. The resulting progeny virions may get some segments from one parent and some from the other. All known segmented virus that infect humans are RNA viruses. The process of reassortment is very efficient in the exchange of genetic material and is used in the generation of viral vaccines especially in the case of influenza live vaccines. The ability of viruses to exchange genetic information through recombination is the basis for virus-based vectors in recombinant DNA technology and hold great promises in the development of gene therapy. Viruses are attractive as vectors in gene therapy because they can be targeted to specific tissues in the organs that the virus usually infect and because viruses do not need special chemical reagents called transfectants that are used to target a plasmid vector to the genome of the host.

Genetic variants generated through mutations, recombination or reassortment could interact with each other if they infected the same host cell and prevent the appearance of any phenotype. This phenomenon, where each mutant provide the missing function of the other while both are still genotypically mutant, is known as complementation. It is used as an efficient tool to determine if mutations are in a unique or in different genes and to reveal the minimum number of genes affecting a function. Temperature sensitive mutants that have the same mutation in the same gene will for example not be able to complement each other. It is important to distinguish complementation from multiplicity reactivation where a higher dose of inactivated mutants will be reactivated and infect a cell because these inactivated viruses cooperate in a poorly understood process. This reactivation probably involves both a complementation step that allows defective viruses to replicate and a recombination step resulting in new genotypes and sometimes regeneration of the wild type. The viruses that need complementation to achieve an infectious cycle are usually referred to as defective mutants and the complementing virus is the helper virus. In some cases, the defective virus may interfere with and reduce the infectivity of the helper virus by competing with it for some factors that are involved in the viral life cycle. These defective viruses called "defective interfering" are sometimes involved in modulating natural infections. Different wild type viruses that infect the same cell may exchange coat components without any exchange of genetic material. This phenomenon, known as phenotypic mixing is usually restricted to related viruses and may change both the morphology of the packaged virus and the tropism or tissue specificity of these infectious agents.

Virus replication. Viral replication refers to the means by which virus particles make new copies of themselves. Although precise mechanisms vary, viruses cause disease by infecting a host cell and commandeering the host cell's synthetic capabilities to produce more viruses. The newly made viruses then leave the host cell, sometimes killing it in the process, and proceed to infect other cells within the host.

Viruses cannot replicate by themselves. They require the participation of the replication equipment of the host cell that they infect in order to replicate. The molecular means by which this replication takes place varies, depending upon the type of virus.

Viral replication can be divided up into three phases: initiation, replication, and release.

The initiation phase occurs when the virus particle attaches to the surface of the host cell, penetrates into the cell and undergoes a process known as uncoating, where the viral genetic material is released from the virus into the host cell's cytoplasm. The attachment typically involves the recognition of some host surface molecules by a corresponding molecule on the surface of the virus. These two molecules can associate tightly with one another, binding the virus particle to the surface. A well-studied

example is the haemagglutinin receptor of the influenzae virus. The receptors of many other viruses have also been characterized.

A virus particle may have more than one receptor molecule, to permit the recognition of different host molecules, or of different regions of a single host molecule. The molecules on the host surface that are recognized tend to be those that are known as glycoproteins. For example, the human immunodeficiency virus recognizes a host glycoprotein called CD4. Cells lacking CD4 cannot, for example, bind the HIV particle.

Penetration of the bound virus into the host interior requires energy. Accordingly, penetration is an active step, not a passive process. The penetration process can occur by several means. For some viruses, the entire particle is engulfed by a membrane-enclosed bag produced by the host (a vesicle) and is drawn into the cell. This process is called endocytosis. Polio virus and orthomyxovirus enters a cell via this route. A second method of penetration involves the fusion of the viral membrane with the host membrane. Then the viral contents are directly released into the host. HIV, paramyxoviruses, and herpes viruses use this route. Finally, but more rarely, a virus particle can be transported across the host membrane. For example, poliovirus can cause the formation of a pore through the host membrane. The viral DNA is then released into the pore and passes across to the inside of the host cell.

Once inside the host, the viruses that have entered via endocytosis or transport across the host membrane need to release their genetic material. With poxvirus, viral proteins made after the entry of the virus into the host are needed for uncoating. Other viruses, such as adenoviruses, herpesviruses, and papovaviruses associate with the host membrane that surrounds the nucleus prior to uncoating. They are guided to the nuclear membrane by the presence of so-called nuclear localization signals, which are highly charged viral proteins. The viral genetic material then enters the nucleus via pores in the membrane. The precise molecular details of this process remains unclear for many viruses.

For animal viruses, the uncoating phase is also referred to as the eclipse phase. No infectious virus particles can be detected during that 10 to 12 hour period of time.

In the replication, or synthetic, phase the viral genetic material is converted to deoxyribonucleic acid (DNA), if the material originally present in the viral particle is ribonucleic acid (RNA). This so-called reverse transcription process needs to occur in retroviruses, such as HIV. The DNA is imported into the host nucleus where the production of new DNA, RNA, and protein can occur. The replication phase varies greatly from virus type to virus type. However, in general, proteins are manufactured to ensure that the cell's replication machinery is harnessed to permit replication of the viral genetic material, to ensure that this replication of the genetic material does indeed occur, and to ensure that this newly made material is properly packaged into new virus particles.

Replication of the viral material can be a complicated process, with different stretches of the genetic material being transcribed simultaneously, with some of these gene products required for the transcription of other viral genes. Also replication can occur along a straight stretch of DNA, or when the DNA is circular (the so-called "rolling circle" form). RNA-containing viruses must also undergo a reverse transcription from DNA to RNA prior to packaging of the genetic material into the new virus particles.

In the final stage, the viral particles are assembled and exit the host cell. The assembly process can involve helper proteins, made by the virus or the host. These are also called chaperones. Other viruses, such as tobacco mosaic virus, do not need these helper chaperones, as the proteins that form the building blocks of the new particles spontaneously self-assemble. In most cases, the assembly of viruses is symmetrical; that is, the structure is the same throughout the viral particle. For example, in the tobacco mosaic virus, the proteins constituents associate with each other at a slight angle, producing a symmetrical helix. Addition of more particles causes the helix to coil "upward" forming a particle. An exception to the symmetrical assembly is the bacteriophage. These viruses have a head region that is supported by legs that are very different in structure. Bacteriophage assembly is very highly coordinated, involving the separate manufacture of the component parts and the direct fitting together of the components in a sequential fashion.

Release of viruses can occur by a process called budding. A membrane "bleb" containing the virus particle is formed at the surface of the cell and is pinched off. For herpes virus this is in fact how the viral membrane is acquired. In other words, the viral membrane is a host-derived membrane. Other viruses, such as bacteriophage, may burst the host cell, spewing out the many progeny virus particles. But many viruses do not adopt such a host destructive process, as it limits the time of an infection due to destruction of the host cells needed for future replication.

FURTHER READING:

BOOKS:

Doerfler, Walter, and Petra Bohm, eds. *Virus Strategies: Molecular Biology and Pathenogenesis.* New York: VCH, 1993.

Flint, S. J., et al. *Principles of Virology: Molecular Biology, Pathogenesis, and Control.* Washington: American Society for Microbiology, 1999.

Kurstak, Edouard, ed. *Control of Virus Diseases.* New York: Marcel Dekker, 1993.

Richman, D. D., and R. J. Whitley. *Clinical Virology.* 2nd ed. Washington: American Society for Microbiology, 2002.

Thomas, D. Brian. *Viruses and the Cellular Immune Response.* New York: Marcel Dekker, 1993.

PERIODICALS:

Peters, C. J., and J. W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix–xvi.

ELECTRONIC:

Biology Pages. "Viruses." 2002. <http://www.ultranet.com/~jkimball/BiologyPages/V/Viruses.htm>l> (April 12, 2003).

SEE ALSO

Bacterial Biology
Biological and Toxin Weapons Convention
Biological Warfare
Biological Weapons, Genetic Identification
Bioshield Project
Bioterrorism
Bioterrorism, Protective Measures

Viral Exposure Therapy, Antiviral Drug Development

BRIAN D. HOYLE

Several National Institute of Health and Defense Department funded programs are currently attempting to develop drugs that can be used to combat viruses most likely to be used by bioterrorists.

Antiviral drugs are compounds that are used to prevent or treat viral infections via the disruption of an infectious mechanism used by the virus, or to treat the symptoms of an infection. In addition to the development of vaccines, researchers are attempting to develop fast action identification and pharmacogenetic protocols for the development of effective anti-viral drugs that could potentially remediate some of the symptoms of viral exposure or early stage infection.

Different types of antiviral drugs have different modes of operation. One specific class of antiviral drugs are known as the antiretroviral drugs. These drugs target those viruses of clinical significance called retroviruses that use the mechanism of reverse transcription to manufacture the genetic material needed for their replication. The prime example of a retrovirus is the Human immunodeficiency virus (HIV), which is the viral agent of acquired immunodeficiency syndrome (AIDS). The development of antiviral drugs has been stimulated by the efforts to combat HIV.

Specific antiviral agents are designed to thwart the replication of whatever virus they are directed against. One means to achieve this is by blocking the virus from commandeering the host cell's nuclear replication machinery in order to have its genetic material replicated along with the host's genetic material. The virus is not killed directly. But the prevention of replication will prevent the numbers of viruses from increasing, giving the host's immune system time to deal with the stranded viruses.

The incorporation of the nucleotide building blocks into deoxyribonucleic acid (DNA) can be blocked using the drug idoxuridine or trifluridine. Both drugs replace the nucleoside thymidine, and its incorporation produces a nonfunctional DNA. However, the same thing happens to the host DNA. So, this antiviral drug is also an anti-host drug.

Blockage of the viral replicative pathway by mimicking nucleosides can also be successful. But, because the virus utilizes the host's genetic machinery, stopping the viral replication usually affects the host cell.

Another tack for antiviral drugs is to block a viral enzyme whose activity is crucial for replication of the viral genetic material. The drug is converted in the host cell to a compound that can out-compete another compound for the binding of the viral enzyme, DNA polymerase, which is responsible for building DNA. The incorporation of the drug into the viral DNA stops the formation of the DNA.

Other antiviral drugs are directed at the translation process, whereby the information from the viral genome that has been made into a template is read to produce the protein product. For example, the drug ribavirin—used to combat the 2003 global Severe Acute Respiratory Syndrome (SARS) pandemic—inhibits the formation of messenger ribonucleic acid.

Still other antiviral drugs are directed at earlier steps in the viral replication pathway (e.g., blocking penetration into the host cell or release of nuclear material).

Antiviral therapy also includes molecular approaches. The best example is the use of oligonucleotides. These are sequences of nucleotides that are specifically synthesized to be complimentary with a target sequence of viral ribonucleic acid. By binding to the viral RNA, the oligonucleotide blocks the RNA from being used as a template to manufacture protein.

The use of antiviral drugs is not without risk. Host cell damage and other adverse host reactions can occur. Thus, the use of antiviral drugs is routinely accompanied by close clinical observation.

FURTHER READING:

BOOKS:

Kurstak, Edouard, ed. *Control of Virus Diseases.* New York: Marcel Dekker, 1993.

ELECTRONIC:

Pan American Health Organization, World Health Organization. Severe Acute Respiratory Syndrome (SARS)

<http://www.paho.org/English/HCP/HCT/EER/sars.htm> (April 6, 2003).

SEE ALSO

Bioshield Project
Bioterrorism, Protective Measures
Viral Biology

Voice Alteration, Electronic

In most cases, voice alteration technologies are employed to obscure an individual's identity. The ability of to alter the voice, however, also can be very useful in intelligence gathering and espionage. Impersonating a target individual (e.g., a worker important in the hierarchy of an organization) can provide access to information that is privy to only a select group of people. As well, if the voice alteration is sufficiently close to the original, access to files or physical locations that are barred by voice recognition software can be granted.

Crude voice alteration can be achieved by physical training. Actors and singers, for example, can train their voices so that the speech or song "projects" to all areas of the theatre. Also, accents can be learned and mimicked with reasonable accuracy.

In this natural process the vocal cords function as the source of the sounds and the vocal tract functions as the filter that can alter the frequency and cadence of the speech. The results is the rising and falling tones and intensity of spoken words.

However, the use of electronic technology can achieve accurate vocal alterations that are not otherwise possible. For example, vocal cords can be trained to be able to adopt different pitches—that is, to be capable of vibrating at different frequencies, so as to produce sounds that have different tones. However, electronic alterations of pitch can widen the vocal deceptions that are possible. For example, a man's voice can be altered to sound absolutely convincingly like a woman's.

The alteration of pitch can also be deliberately done electronically by detecting the frequency pattern of the speaker, and of the particular phrase being spoken. On a screen, the pattern appears as a series of waves and troughs. The arrangement of the waves and troughs is characteristic to the word being spoken. For example, the word "cat" will produce a different pattern than the word "invisible." By applying an electronic filter (or "window"—actually one or more mathematical equations, or algorithms) to the frequency pattern, waves and troughs can be selectively eliminated or shifted up and down to produce a different frequency. An experienced technician or sophisticated software program can alter a word so as to change the sound of the word (i.e., a higher or lower tone) without distorting the sound of the word. Thus, the altered speech is still recognizable and interpretable, but can sound like it is being spoken by another person.

Electronic voice alteration can be subtle or extreme. The latter is associated with the almost incomprehensible voices of anonymous witnesses. This type of voice alteration is actually a voice disguise. The intention is not to mimic a voice, but to scramble the voice patterns to make the identify of the speaker impossible to identify.

There are several different electronic means of voice alteration. One type is known as speech inversion. Here, the frequency signal is in effect turned inside out around a designated frequency. Put another way, the parts of the speech that are "high" are made to sound "low", and visa versa.

A voice can also be electronically jumbled, so that it sounds like gibberish. But codes assigned to sections of the speech allows the listener (who has the electronic codes) to put the words back in their proper order.

Another means of electronic voice alteration is known as speech encryption. Here, speech is digitized and the digital signal manipulated to make the text of the speech unrecognizable to the listener's ear. But, the speech can be decoded, or decrypted, at the receiving end to yield the original recognizable speech.

Hardware and software voice encryption systems are available. Machines connected to a telephone can alter a person's speech during the telephone conversation. Anyone eavesdropping on the conversation would be incapable of understanding what was being said. However, a legitimate listener, having a machine on his or her phone, would be capable of decrypting the conversation.

The United States government and military uses a telephone conversation scrambling software program and hardware called STU III (Secure Telephone Unit, Generation III).

Scrambling digital electronic information in relation to time can also accomplish voice alteration. An example includes the delay of information. While an effective means of altering a voice, the method can produce an echo, and so is unpleasantly distracting to listen to.

FURTHER READING:

BOOKS:

Hollien, Harry Francis. *The Acoustics of Crime: The New Science of Forensic Acoustics.* New York: Plenum Press, 1990.

———. *Forensic Voice Identification.* New York: Academic Press, 2001.

SEE ALSO

Cryptology, History

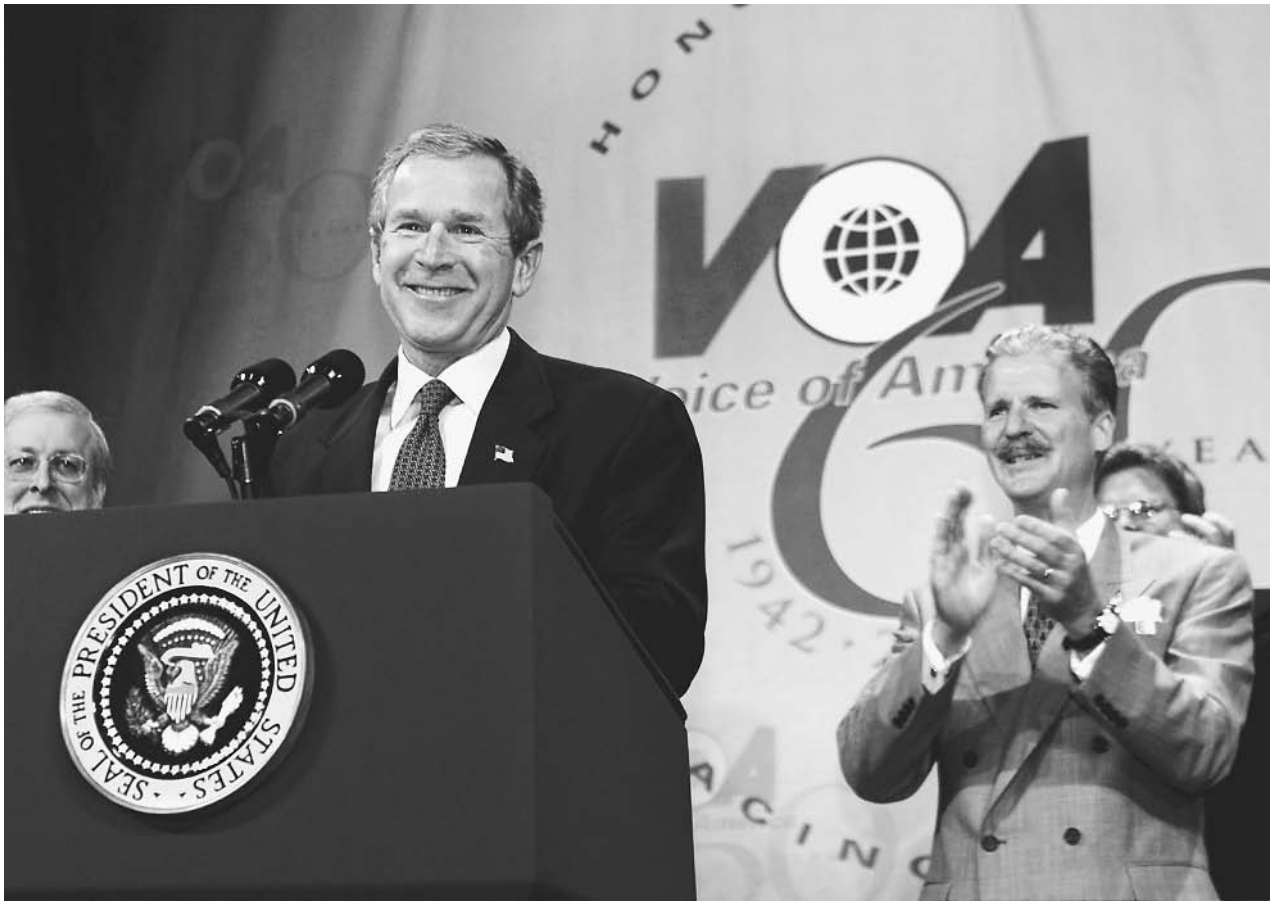
Electro-optical Intelligence
Parabolic Microphones

Voice of America (VOA), United States

CARYN E. NEUMANN

The Voice of America (VOA) is a radio, television, and Internet news service that serves as the non-military voice of the United States government by communicating a comprehensive account of America and the world directly to people in other nations. Prohibited by law from broadcasting into the U.S., VOA uses 53 languages while transmitting more than 1,000 hours of news, informational, educational, and cultural programming every week from its Washington, D.C. headquarters to a worldwide audience of about 94 million people. Although the aim of VOA is to promote the long-range interests of Americans, the news service is separated from the U.S. government by a firewall. It does not officially speak for the U.S. government, accepts no special treatment or assistance from American officials or government organizations, and strives for balanced and accurate news reporting. Separate sister agencies of VOA include Radio Free Europe, Radio Free Asia, and the Cuba-focused Radio Martí, with all of these information services overseen and guided by the Broadcasting Board of Governors.

VOA has evolved since its 1942 creation from an agitprop instrument that demanded action from its listeners to a news organization that calmly presents a balanced portrait of current events. In the 1930s, every major world power, especially that of Germany, capitalized on radio's potential to influence public opinion. The U.S., at that time less interested in playing a role in world affairs, did not see the value in developing a system of international radio propaganda. The fall of France, created in part by Nazi Germany's use of propaganda to destroy the French will to fight, changed U.S. opinion. President Franklin D. Roosevelt realized that ideas could be as useful as tanks in a military effort and he began to mobilize for propaganda



President Bush marks the 60th anniversary of Voice of America, a service that relays news to the world in 53 languages by radio, TV, and the Internet, at a celebration at VOA headquarters in Washington, D.C., in February 2002. AP/WIDE WORLD PHOTOS.

warfare. In 1941, Roosevelt established the U.S. Foreign Information Service (FIS) and the first U.S. government-sponsored radio broadcast was delivered on February 24, 1942 from New York City to Europe. In June 1942, the government established the Overseas Branch of the Office of War Information and six months later Roosevelt authorized the operation of VOA. The first VOA director, John Houseman, was an actor and playwright who used his dramatic skills to create agitprop. Under Houseman, every tone emanating from a VOA broadcast urged the French to join the resistance against the Nazis. Following the November 1942 Allied invasion of North Africa, VOA shifted its delivery style to calm and neutral news reporting that focused on the impending Allied liberation of Europe rather than the need for resistance.

The VOA seemed to be unnecessary once World War II had ended, but the start of the Cold War combined with hostile international broadcasting by the Soviet Union to make the news service into a valuable tool of democratic views. On August 1, 1953, VOA moved from its post-war location within the Department of State to join the newly formed U.S. Information Agency. The number of broadcasts delivered by VOA rose dramatically as the agency responded to the information needs of people behind the Iron Curtain and in politically unstable countries. In 1959, VOA inaugurated Special English, a slow-paced broadcast of simplified English for non-native speakers that was designed to facilitate comprehension. In 1994, VOA entered the television market with a Chinese-language program beamed by satellite. In 1996, VOA television studios were completed and the agency now simulcasts some portions of its programming on both radio and television in twelve languages: Albanian, Arabic, Bosnian, English, Indonesian, Mandarin Chinese, Persian, Russian, Serbian, Spanish, and Ukrainian. It also provides programming to 1200 radio stations around the world.

VOA's ability to broadcast consistently reliable and authoritative news to people in closed and war-torn societies makes it a valuable component of American security and intelligence efforts. Although it has occasionally come under attack by political leaders for failing to promote the overthrow of undemocratic governments, critics contend that VOA has succeeded in its mission of delivering unbiased news to a wide audience.

FURTHER READING:

BOOKS:

Fitzgerald, Merni Ingrassia. *The Voice of America.* New York: Dodd, Mead, 1987.

Piresein, Robert William. *The Voice of America: A History of the International Broadcasting Activities of the United States Government 1940–1962.* New York: Arno Press, 1979.

Shulman, Holly Cowan. *The Voice of America: Propaganda and Democracy 1941–1945.* Madison: The University of Wisconsin Press, 1990.

ELECTRONIC:

Voice of America. "About VOA." February 1, 2003. <http://www.voa.gov/index.cfm> (February 1, 2003).

SEE ALSO

Cold War (1950–1972)
Department of State, United States
Information Warfare

Vozrozhdeniye Island, Soviet and Russian Biochemical Facility

BRIAN HOYLE

Vozrozhdeniye Island is a Russian island located in the Aral Sea approximately 1,300 miles to the east of Moscow that was used as a bioweapons test facility for the former Soviet Union. Since being decommissioned in the early 1990s the island has been left virtually unpatrolled. The island has served for decades as the repository of a large quantity of spores of *Bacillus anthracis*, the bacterial agent of anthrax, and other disease-causing bacteria and viruses. As the surrounding water has receded over the decades, direct access from the mainland to the island, and to the stocks of bioweapons that were disposed of by being buried on the island, will soon be possible. Concern is growing in the international community that the island will become a source of a new generation of bioweapons.

During its operation, the bioweapons facility on Vozrozhdeniye Island was regarded as an important strategy of the former Soviet Union in the tensions between the East and the West during the Cold War of the 1950s. Indeed, the word Vozrozhdeniye translates in Russian as "renaissance."

The island was used for open-air testing of bioweapons. The island was selected for its remote location and harsh conditions. The sparse vegetation and summer temperatures that reached 140 degrees Fahrenheit created inhospitable conditions that lessened the chances of survival for microorganisms that escaped. Records obtained following the island's decommissioning confirm that anthrax weapons were tested. As well, other microorganisms that were tested for their potential in biological warfare include the microbial agents of tularemia, plague, typhoid, and possibly smallpox.

The anthrax buried on the island was designed especially for the lethal use on humans in the time of war. The powder is a freeze-dried form of *Bacillus anthracis* called a

spore. A spore is a form of the some species of *Bacillus* and *Clostridium* that protects the organism's genetic material during times when conditions are not favorable for the survival of the actively growing form of the bacterium. Bacterial spores that are capable of resuscitation and growth have been recovered from samples over 100 years old. Resuscitation of the spore requires only suspension in growth media having the appropriate nutrients and incubation of the suspension at a temperature that is hospitable for the bacterial growth.

Following the banning of offensive biological weapons programs in the United States and Russia, the biological warfare agents on Vozrozhdeniye Island were buried on the island in 1988. The island was abandoned in 1991.

Vozrozhdeniye island has remained unguarded since 1991. Then, it was thought that the island's location in the middle of the large and geographically isolated Aral Sea made the island secure from entry. However, in the intervening decades the demands for irrigation water have caused the Aral Sea—the largest freshwater lake in the world—to be used as a source of irrigation water. Water has consistently been withdrawn faster than it can be replenished. As a result, the water level of the Aral Sea has declined drastically, so much so that many scientists now fear that Vozrozhdeniye Island might soon be directly connected to the mainland. If so, and if the island remains unguarded, the buried stockpiled weapons could be vulnerable to theft.

Additionally, some surveys of the island have indicated that migration of some of the buried material towards the surface is occurring. Upon surface exposure, the bacteria and viruses, which may still be capable of infection, could be spread in the wind or transported elsewhere by birds.

■ FURTHER READING:

PERIODICALS:

Choffnes, E. "Germs on the Loose." *Bulletin of the Atomic Scientists* no. 57 (2001): 57–61.

ELECTRONIC:

Monterey Institute of International Studies. "Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future." CNS Occasional Papers. 2002. <http://cns.miis.edu/pubs/opapers/opl/opl.htm#island>(28 December 2002).

National Aeronautics and Space Administration. "Rebirth Island Joins the Mainland." Earth Observatory. <http://earthobservatory.nasa.gov/Newsroom/NewImages/images.php3?img_id=5108>(27 December 2002).

SEE ALSO

Biocontainment Laboratories
Bioterrorism, Protective Measures
Russia, Intelligence and Security

Vulnerability Assessments

As its name suggests, a vulnerability assessment is a test of a system to locate, diagnose, and correct areas of weakness that might make it susceptible in times of crisis, attack, or destabilization. Any system that is created, operated, and shaped by humans may qualify for, and may in fact require, a vulnerability assessment. The expression entered the English language in the 1980s and 1990s, and usage increased markedly after the terrorist attacks of September 2001. Vulnerability assessments have been applied to everything from computer networks to water systems.

In 1998 and 1999, Sandia National Laboratories in Albuquerque, New Mexico, in partnership with the National Law Enforcement and Corrections Technology Center-Southeast Region, assessed the vulnerability of several correctional facilities. The first step in such an assessment was to determine areas of vulnerability, and then to examine scenarios whereby those vulnerabilities are exploited. In the case of the prisons, the partnership examined classes of adversaries, including inmates and their families, along with tactics they might use, as well as all reasonable escape scenarios. It was noted that, rather than using a checklist in the design of prison security, it was advisable to apply a more advanced computer-driven analysis system. This would make it possible to consider all available means by which adversaries might achieve their objectives.

In June 2002, the nation's 54,000 drinking water systems and 16,000 wastewater agencies spent a combined $700 million on vulnerability assessments, many of which had been spurred by the terrorist attacks of the preceding fall. At the same time, the Environmental Protection Agency (EPA) and the newly created Office (now Department) of Homeland Security had called for vulnerability assessments of critical infrastructure nationwide. Some industries welcomed this call as an opportunity for new business, but members of the oil and gas industry lobbied against a plan whereby companies would conduct vulnerability assessments and the EPA would assess compliance in certain areas. Meanwhile, vulnerability assessments have remained a powerful topic in the world of computers and cybersecurity. In January 2003, for instance, the Chemical Industry Date Exchange announced the formation of a new cybersecurity unit that would conduct a vulnerability assessment of chemical companies.

■ FURTHER READING:

PERIODICALS:

"EPA Security Plan for Refining, Chemical Plants Blasted." *Oil & Gas Journal* 100, no. 39 (September 23, 2002): 22–24.

Giodano, Vincent. "Is It Right for Your Company?" *Communications News* 37, no. 9 (September 2000): 66–68.

Landers, Jay. "Safeguarding Water Utilities." *Civil Engineering* 72, no. 6 (June 2002): 48–53.

Seewald, Nancy. "CIDX Forms Cybersecurity Unit." *Chemical Week* 165, no. 2 (January 15, 2003): 20.

Spencer, Debra D. "Vulnerability Assessment." *Corrections Today* 60, no. 4 (July 1998): 88–92.

Wright, Andrew J., et. al. "War, Recession, and Growth." *ENR* 249, no. 2 (July 8, 2002): 34–36.

SEE ALSO

Critical Infrastructure
Terrorism, Intelligence Based Threat and Risk Assessments

VX Agent

JULI BERWALD

VX nerve agent (O-ethyl S-[2-diisoproylaminoethyl] methylphsophonothioate) is one of the most toxic substances ever developed. Like other nerve agents, it is an organophosphate. Although it is often called a nerve gas, VX is usually a clear, odorless, tasteless liquid. A tiny amount of VX, about 10 mg—absorbed through the skin or eyes is fatal—and death usually occurs within an hour of exposure. VX poisons by binding to the enzyme cholinesterase and inactivating it. As a result, the chemical signals passed between nerve cells are transmitted uncontrollably. Symptoms of VX poisoning include constriction of the pupils, headache, runny nose, nasal congestion, chest tightness, giddiness, anxiety, and nausea, eventually progressing to convulsions and respiratory failure. VX poisoning can be treated immediately with two antidotes: atropine and pralidoxome chloride. Because of its extreme toxicity, VX is considered a weapon of mass destruction.

VX poisoning. Chemical signals are transmitted between nerve cells by means of small molecules called neurotransmitters. One of the most common neurotransmitters in the central and peripheral nervous system is acetylcholine. Under normal conditions, acetylcholine is released from the terminal axon of one nerve cell, crosses the synaptic cleft between nerve cells and binds with a receptor on the membrane of the post-synaptic nerve cell. Then, the enzyme cholinesterase binds to acetylcholine and inactivates it. This completes the chemical signaling between nerve cells.

When the VX nerve agent is present in the nervous system, it inactivates the enzyme cholinesterase. As a result, the receptor on the post-synaptic nerve cell is indefinitely stimulated by acetylcholine. In addition, the pre-synaptic nerve cell continues to release acetylcholine. Nervous signals are never completed and the nervous system is eventually destroyed.

VX poisoning can occur by exposure to the eyes or skin, inhalation, or ingestion. Symptoms occur within minutes. Autonomic nervous system symptoms include constricted pupils, reduced vision and other visual effects, drooling, sweating, diarrhea, nausea, vomiting, and abdominal pain. Neuromuscular symptoms are twitching, weakness, paralysis, and eventually respiratory failure. Symptoms affecting the central nervous system are headache, confusion, depression, convulsions, coma, respiratory depression, and respiratory arrest.

Treatment of VX poisoning. Two antidotes exist for VX poisoning: atropine and pralidoxime chloride, also called 2-PAM. Atropine blocks one type of acetylcholine receptor on the post-synaptic nerve cell membrane. This prevents acetylcholine that is in the synaptic cleft from binding to the receptor. Pralidoxime chloride prevents VX from binding to cholinesterase. Together, these drugs have been combined in an antidote kit called Mark I. Mark I is issued to United States troops, in particular those serving in the Persian Gulf region. Diazepam can also be used to treat the seizures and convulsions that may occur as a result of VX poisoning.

If VX is exposed to the eyes, they should be flushed with water for 10 to 15 minutes. Skin contact should be treated with washing in soap and water, 10% sodium carbonate solution or 5% bleach solution. If sweating and muscular twitching occur, then Mark I should be administered. If VX is ingested, Mark I should be injected immediately.

The history of VX. VX nerve agent was developed in 1952 by British chemists who were researching different types of insecticides. The United Kingdom traded information about VX with the United States government in exchange for information about thermonuclear weapons in 1953. A program to thoroughly study VX was subsequently begun at the Department of the Army's Edgewood Arsenal in Maryland. In 1957, scientists at Edgewood developed a binary system for delivery of VX in weapons. During the 1960s or 1970s, the Soviet Union's intelligence agencies learned the formula for VX and soviet scientists developed a program for the mass production of VX.

Although VX has not yet been used as a weapon, in 1968, the U.S. Army experimented with open-air tests of weapons containing VX at Dugway Proving Ground near Salt Lake City in Utah. During a test on March 14, a valve failed on an aircraft carrying the nerve gas and 320 gallons of VX were inadvertently sprayed over fields. Subsequently, 6,400 sheep that were grazing in the area died. The Army eventually took responsibility for the mishap and reimbursed ranchers for their loss.

The Iraqi government has admitted to manufacturing VX during the 1990s. It is possible that the formula for

producing VX could have passed to Iraq via Russia, however the U.S. government has found no solid evidence of such a transfer of information. Further, reports surfaced in 2002 that the al-Qaeda terrorist network has obtained VX, but they had not been substantiated as of early 2003.

The use of VX as a weapon. VX is an extremely toxic material with low volatility and therefore, it dissipates very slowly. VX also has adhesive properties, which makes it difficult to remove from surfaces. These characteristics make a powerful strategic contaminant. For example, military bases contaminated with VX could result in casualties for several weeks if the base continued to be used. In order to counter such tactics by terrorist groups, scientists at the Department of Energy's Idaho National Engineering and Environmental Laboratory have recently developed technology to detect VX and to predict its degradation rate on concrete surfaces. Because of its potent toxicity, if VX were used on a missile, it could be an extremely deadly weapon. The LD50, or lethal dose for at least 50% of those exposed to VX is 10 ml. Therefore, VX is considered a weapon of mass destruction.

FURTHER READING:

BOOKS:

Haugen, David M., editor. *Biological and Chemical Weapons.* San Diego: Greenhaven Press, Inc., 2001.

Seagrave, Sterling. *Yellow Rain: A Journey through the Terror of Chemical Warfare.* New York: M. Evans and Company, Inc., 1981.

Sifton, David W., editor. *PDR Guide to Biological and Chemical Warfare Response.* Montvale, NJ: Thompson/Physician's Desk Reference, 2002.

Wise, David. *Cassidy's Run: The Secret Spy War over Nerve Gas.* New York: Random House, Inc., 2000.

ELECTRONIC:

Chemical Weapons: Nerve Agents. <http://faculty.washington.edu/chudler/weap.html> (February 11, 2003).

Material Safety Data Sheet: Lethal Nerve Agent VX. <http://www.ilpi.com/msds/vx.html> (February 11, 2003).

United States Army. Chemical Agent Fact Sheet: VX. <http://www.sbccom.army.mil/services/edu/vx.htm> (February 11, 2003).

SEE ALSO

Chemical Warfare
Toxins

This page intentionally left blank

Walker Family Spy Ring

John Anthony Walker, a United States citizen, successfully spied on behalf of the Soviet KGB from 1967 to 1985. Walker employed friends and members of his family in the business of espionage, stealing secrets from U.S. Naval Intelligence and selling them to Soviet agents. During the course of his career, Walker compromised United States military communications ciphers, copied blueprints of Naval vessels and weapons, and stole secret documents.

In 1984, Walker's ex-wife, Barbara Crowley Walker, tipped FBI investigators to her husbands dealings with the Soviets. She told investigators that she suspected he did not work alone, and most likely relied on his brothers and a friend to steal government secrets.

The FBI conducted extensive surveillance of Walker for several months, trying to catch him in the act of leaving information at pre-arranged dead drop for a Soviet agent to retrieve. In April 1985, investigators learned of Walker's plans to leave documents at a dead drop site in Maryland, in exchange for a sizable cash payment to be picked up from another location. On May 19, 1985, FBI agents watched Walker leave a crumpled paper sack near a roadside utility pole. After Walker left the site to drive one hour north to receive his payment, agents seized the dead drop materials, 129 top secret Navy intelligence documents.

Walker then went to the second site to pick up the dead drop a Soviet agent left for him, $200,000 in cash. However, the bag containing the money was not at the site. After searching for nearly two hours, Walker left the drop site and checked into a local motel, worried that the FBI may have compromised the transaction. Walker was arrested outside his hotel room later the same night.

Despite warnings from his handlers in the KGB, Walker included personal letters and information in his last few dead drops. When the FBI seized Walker's last drop, the package contained not only the stolen secret documents but also a letter containing the names of other members of his spy ring. The names appeared in code, but FBI and CIA personnel readily identified the cryptonym. Walker's own writing implicated his son, Michael Lance Walker, a seaman stationed aboard the USS *Nimitz*. Michael Walker supplied his father with many of the documents, photographs, and code information that his father sold to Soviet agents. All 129 stolen documents in Walker's final dead drop were stolen by his son.

Walker's letters also noted the involvement of his older brother, Arthur Walker, in the activities of the spy ring. Arthur was a Navy veteran and a defense contractor, privy to information about weapons systems and ship and aircraft design.

Jerry Alfred Whitworth, Walker's best friend and a Navy communications specialist, operated in the spy ring for over ten years. Whitworth supplied Walker with most of the United States cipher and code information leaked to the Soviets.

Walker, his son, and Whitworth were tried on charges of espionage. Walker received life in prison, while Michael and Whitworth received lesser sentences. Walker's son, Michael, was released from prison in 2000.

Although Moscow celebrated Walker as one of their best recruits, Walker's arrest served as a catalyst for a widespread investigation of security procedures within the United States intelligence community. A year after Walker's arrest, investigators and intelligence officials exposed seven other suspected double agents operating against the United States.

FURTHER READING:

ELECTRONIC:

The Center for Counterintelligence and Security Studies. <http://www.cicentre.com> (April 2003).

SEE ALSO

Ames (Aldrich H.) Espionage Case

Dead Drop Spike
Dead-Letter Box
FBI (United States Federal Bureau of Investigation)
Hanssen (Robert) Espionage Case
*KGB (*Komitet Gosudarstvennoi Bezopasnosti*, USSR Committee of State Security)*
Russia, Intelligence and Security

War of 1812

ADRIENNE WILMOTH LERNER

The War of 1812, spawned by the European Napoleonic Wars, was the last war in which the fledgling United States fought its former colonial power, Great Britain. After three years of fighting on land and at sea, the United States military successfully drove the British forces from United States soil, but not before British troops burned Washington, D.C. The War of 1812 assured the United States the independent sovereignty it claimed after victory in the American Revolution and shaped American foreign policy for over a century.

When continental Europe erupted in conflict in 1793, the United States declared itself neutral. Not wanting to anger France or Britain, the two main rivals in the European war, the United States tried to remain out of contentious European politics, especially in regards to European colonial holdings in the Americas. Relations were further strained by British resentment of ongoing United States trade and diplomatic cooperation with France. British ships blockaded United States ports, hoping to prevent supplies and trade goods from reaching France. United States leaders, George Washington and John Adams, worked to ease tensions and lift the blockade, and by 1795, the nation again conducted trade with allies in Europe. However, by 1803, the United States government grew deeply concerned about the presence of a strong British military force in the Great Lakes region. Negotiations with Britain to reduce their military presence in the West and along the northern border of New England failed. Tensions again mounted when France sold the United States significant territories, including the Mississippi River, in the Louisiana Purchase.

In 1805, the British Navy resumed its blockade of the Unites States coast, prohibiting the export of most goods to continental Europe. The Orders in Council of 1807 further restricted neutral trade with Europe, and authorized British ships to take both the cargo and crew of seized neutral ships. The practice of impressment, forcing captured seamen into service on British ships, inflamed anti-British sentiment in the United States. The passage of the Embargo Act, confining all United States trade to the North American coast, the failure of continued diplomatic relations, and British-incited Indian attacks on United States outposts, gave credence to the opinions of the "War Hawks" in the United States government. In June 1812, the United States declared war on Britain.

The War of 1812 forced the United States to rapidly form and train military forces. After the Revolutionary War, the federal government only reluctantly allowed provisions for national forces. Most armies were maintained by individual states, with little standardization of training and equipment. The war spanned the entire breadth of the United States and its territories, from the Great Lakes region to New Orleans, Louisiana. Regional armies facilitated troop movement and deployment, but the lack of national infrastructure made travel and communication among the different battlefronts difficult. Military generals attempted to create a complex communication and espionage network, utilizing couriers on horseback and semaphore, to deliver messages. Codes were primitive and easy to break, but both British and American forces employed invisible inks to help conceal communications.

The vast expanses of rough and unfamiliar territory that both armies traversed required the extensive use of scouts. Both British and American forces preferred to use Indian scouts, who often had superior knowledge of regional terrain and could communicated in several indigenous languages. Indian scouts also aided in the recruitment of Indians to fight rival forces. British and United States military leaders also attempted to spark warfare between rival tribes with varying allegiances, hoping to distract opposing forces or break their aid network. Extensive contact with indigenous populations proved devastating, as during the American Revolution, disease ravaged Indian villages and several thousand Indian warriors died in battle.

From 1812 to 1814, the United States suffered numerous crushing defeats at the hands of superior British forces. United States offensives failed to take the Great Lakes region, and military defenses could not keep British troops from occupying Washington, D.C. Anticipated French aid never materialized in the 1813, as the tide of war in Europe had shifted decisively in favor of the British, and Napoleon's French Empire was in grave danger of collapse. American diplomats in Paris maintained a small espionage network in Europe and the Americas to monitor the British military and diplomatic corps. A French spy, posing as a local trader, rode to the White House to inform the president and cabinet members of the British plans to invade, occupy, and then destroy Washington, D.C. The government fled the British invasion of the capital city, but only by a matter of hours.

Despite the grim prospects of the United States land campaign in the early years of the war, the new United States Navy mounted surprisingly successful battles against the powerful British Navy. The United States reluctantly formed its Navy to combat the extortionist trade monopoly of the North African Barbary Pirates who dominated shipping in the Mediterranean. While wealthier European government simply paid annual tributes and occasional ransoms to the Barbary authorities, the fledgling United States Federal government could not afford to pay such

large sums of money. The nation mounted a small but highly effective Navy, eventually driving the Barbary authorities to capitulation. After the conflict, the government only narrowly voted to keep naval forces.

When the British began the blockade of the American coastline, United States navy and merchant ships successfully ran the blockade. The government employed "pirate" ships to destroy British ships, and recapture seized cargo and Americans impressed into service. With the outbreak of war, naval resources were increasingly devoted to strategic sea campaigns against British vessels. The United States Navy successfully captured the British frigate *Macedonian*, defeated the *Java*, and raided several other merchant and military ships. Victories at sea, though limited, enforced the need for a permanent navy in the United States and ensured its continued survival. One hundred and forty years later, the United States Navy surpassed the British fleet to become the world's dominant sea power.

As the French were defeated in Europe, the British devoted more resources to the battlefront in America. However, United States forces rallied, turning the tide of the war in their favor by August 1814. Wishing to avoid clear military defeat, both sides began peace negotiations. The British failure to capture Baltimore prompted the government to settle their dispute with the United States, instead of continuing a lingering, expensive, and increasingly stalemated overseas war. The Treaty of Ghent formally ended the war in 1815. On January 8, 1815, after the signing of the treaty, United States forces, commanded by Andrew Jackson, achieved a stunning victory against the British at the port of New Orleans. Since communication was tedious across the Atlantic and the expansive western territory of Louisiana, news of the Treaty of Ghent did not reach either forces in time to prevent the engagement. The Battle of New Orleans gave the impression that the long-stalemated war was a sound United States victory, but the new nation was successful largely because of the failure of British offensive operations.

After the War of 1812, the United States declared firmer international policy. With the issuance of the Monroe Doctrine in 1823, the nation stated its policy of non-intervention in European conflicts. Furthermore, the United States declared the New World closed to further colonization, and that attempts of foreign powers to intervene in conflicts between colonial powers and their colonies would be viewed as an act of aggression. The War of 1812 solidified the political and military preeminence of the United States in the Americas, and began the great expansion westward toward the Pacific coast.

FURTHER READING:

BOOKS:

Dudley, Wade G. *Splintering the Wooden Wall: The British Blockade of the United States, 1812–1815,* reprint ed. Annapolis, MD: U.S. Naval Institute, 2000.

Hickey, Donald R. *The War of 1812: A Forgotten Conflict.* reprint ed. Champaign, IL: University of Illinois Press,1990.

Katcher, Philip R. *The American War, 1812–1814 (Men-at-Arms, no. 226).* reprint ed. Buffalo, MN: Osprey Publishing, 1990.

SEE ALSO

Revolutionary War, Espionage and Intelligence

Water Supply: Counter-Terrorism

BRIAN HOYLE

The water supply in many communities in the developed world comes from a surface water source such as a lake. Water can also be pumped from aquifer located underground. Typically, the water is routed to a treatment plant, where a variety of physical and chemical processes render the water safe to drink. The "finished" water is then pumped through pipes (i.e., the distribution system) to the consumer's taps.

For over a century this process has been geared toward providing high quality water, without consideration of the security of the acquisition, treatment, and distribution of water. However, particularly since the 1990s, the threat of a deliberate contamination of water supplies has become more probable.

In the wake of the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon in the United States, surface water supplies, water treatment plants, and distribution systems were quickly recognized as potential targets of a terrorist attack. While water facilities are often equipped to discourage mischief (i.e., a chain link fence surrounding a reservoir), virtually no water facilities are designed to prevent a deliberate and coordinated attack.

Many compounds dissolve in water and microorganisms are so small that, for example, up to 6 million bacteria need to be present in each milliliter of water before the water will appear less than crystal clear. Thus, the addition of a lethal quantity of a potent poison or disease-causing microorganism to a water supply could be done without attracting undue notice.

During the 1990s, and especially since the events of September 11, 2001, efforts to develop effective strategies to counter a terrorist attack on water supplies have been widely debated.

The fact that major urban systems need to supply huge quantities of drinking water every day could already be a counter-terrorist strategy. Even given the ease by

which a reservoir could be contaminated, the large volume of the water reservoirs of major urban centers would dilute the added poison to very low levels. A lethal dose of a poison at the consumer's tap would require the addition of a huge amount of the contaminant. For example, it has been estimated over 400,000 metric tons of hydrogen cyanide would have to be added to the Crystal Springs Reservoir—a major reservoir for the city of San Francisco—to supply enough poison to kill or debilitate someone drinking one glass of water from the reservoir.

However, smaller reservoirs are at risk, as are smaller water tanks. Increased security at treatment plants would be an effective deterrent to sabotage. However, such security would be expensive and the cost would be passed to the consumer.

In most municipalities, water treatment involves the addition of chlorine or chlorine products to kill microorganisms. The deliberate disabling of the chlorination system of a treatment plant would make contamination of the drinking water a certainty. For example, a breakdown in the chlorination of the drinking water of Walkerton, Ontario, coincident with the run-off from a cattle field that contaminated the water supply with *Escherichia coli O157:H7*, sickened over 2,000 people and killed at seven people in the summer of 2000.

Even a secure treatment facility supplying chlorinated water is no guarantee of safe water. Recent history has shown that chlorinated water is susceptible to contamination by microorganisms that are resistant to the chemical. Specifically, the protozoa called *Giardia* and *Cryptosporidium* have a spore-like stage in their life cycles that survives exposure to chlorine. A *Cryptosporidium* contamination of the water supply of Milwaukee, Wisconsin, sickened over 200,000 people and killed almost 100 people.

While illness outbreaks with the protozoa have so far been accidental, the use of the microorganisms as a weapon is conceivable. In the United States, municipalities have been legislated to provide alternate means of dealing with drinking water to counter the threat posed by *Giardia* and *Cryptosporidium*. This legislation has been prompted by health concerns. Nonetheless, it will prove to be a counter-terrorism measure.

The distribution system that carries water from the treatment plant to the consumer's taps is another potential target of terrorism. The high pressure inside the pipes would make the introduction of a contaminant difficult. However, the lack of security along the distribution system could enable a dedicated group to commission the digging equipment needed to uncover a pipe and stop water flow long enough to contaminate the water.

Patrolling a distribution system is impossible. For now, the most effective counter-terrorism strategy is to make manholes and storage tanks inaccessible.

Another microbial terrorist threat to drinking water is *Bacillus anthracis*. This bacterium, which is the cause of anthrax, can form a very hardy structure known as a spore. Studies have determined that the spore form can survive in chlorinated water for at least two years. If ingested in a glass of drinking water, or inhaled in the humid environment of a shower or bath, the spores can revive, and the growing bacteria can cause the disease.

Other chlorine-resistant microorganisms that have been identified as bioterrorism agents include *Clostridium perfringens*, *Yersinia pestis* (the cause of plague), and biotoxins (e.g., aflatoxin and ricin).

Countering the deliberate use of such microorganisms will necessitate the rapid detection of even tiny quantities of the microorganisms or their toxic products. Use of rapid detection devices in an early warning system would be an effective counter-terrorism strategy, albeit one that would require dedicated personnel or hardware to monitor the water system.

One promising technology is the use of an electronic sensor ("the electronic nose") to detect chemicals. This method has been successful in detecting spoilage and disease causing bacteria present on fruit by virtue of the unique chemical compounds given off by the bacteria. However, the electronic nose would have to be adapted for use with water.

A detection method that already successfully detects and identifies bacteria such as *Escherichia coli* in fresh water relies on the binding of fluorescent antibodies to the surface of the bacteria and the detection of the bound antibodies by the resulting fluorescence. A prototype of the device is portable and so can be taken to hydrants for the testing of water throughout a distribution system. When in production within the next several years, the device will offer a means of rapidly monitoring water for contaminants.

Another promising technology relies on the recovery of genetic material (deoxyribonucleic acid; DNA) from the sample, and the detection of sequences of the DNA that are unique to the target bacteria by the use of a mirror image piece of DNA that will selectively bind to the target sequence. DNA microchips utilize this technique to detect bacteria from samples as complex as soil and ocean water.

Thus, there is potential for the development of rapid tests to detect bacterial contamination of drinking water. Whether the benefits of implementing an early warning system of chemical and microorganism detection will justify the costs remain to be determined.

In the short term, the best counter-terrorism strategy for many water systems will continue to involve a survey of the system in order to identify points where the system is vulnerable (i.e., unlocked hydrants) and taking action to secure those points (i.e., locking hydrants). As well, public notification of water contamination, and response of authorities (e.g., police, fire department, and medical personnel) to a contamination should be an integral part of a community's emergency response plan.

Despite the vulnerability of water to deliberate contamination, the reality continues to be that the probability of such action is very low. A terrorist can deliver a lethal

payload by air or through routes like the postal system more easily and using less microorganisms than would be required for the contamination of a water supply.

FURTHER READING:

BOOKS:

Lesser, Ian O., and Bruce Hoffman. *Countering the New Terrorism.* Santa Monica: Rand Publications, 1999.

PERIODICALS:

Betts, K. S. "DNA chip technology could Revolutionize Water Testing." *Environmental Science and Technology* no. 33 (1999): 300A–301A.

Burrows, W. D., and S. E. Renner. "Biological Warfare Agents as Threats to Potable Water." *Environmental Health Perspectives* no. 107 (1999): 975–84.

Foran, J. A., and T. M. Brosnan. "Early Warning Systems for Hazardous Biological Agents in Potable Water." *Environmental Health Perspectives* no. 108 (2000): 993–96.

Weckerle, J. F. "Domestic preparedness for events involving weapons of mass destruction." *Journal of the American Medical Association* no. 283 (1997): 435–38.

SEE ALSO

Biological Warfare
Chemical Warfare
Pathogen Transmission
United States, Counter-terrorism Policy

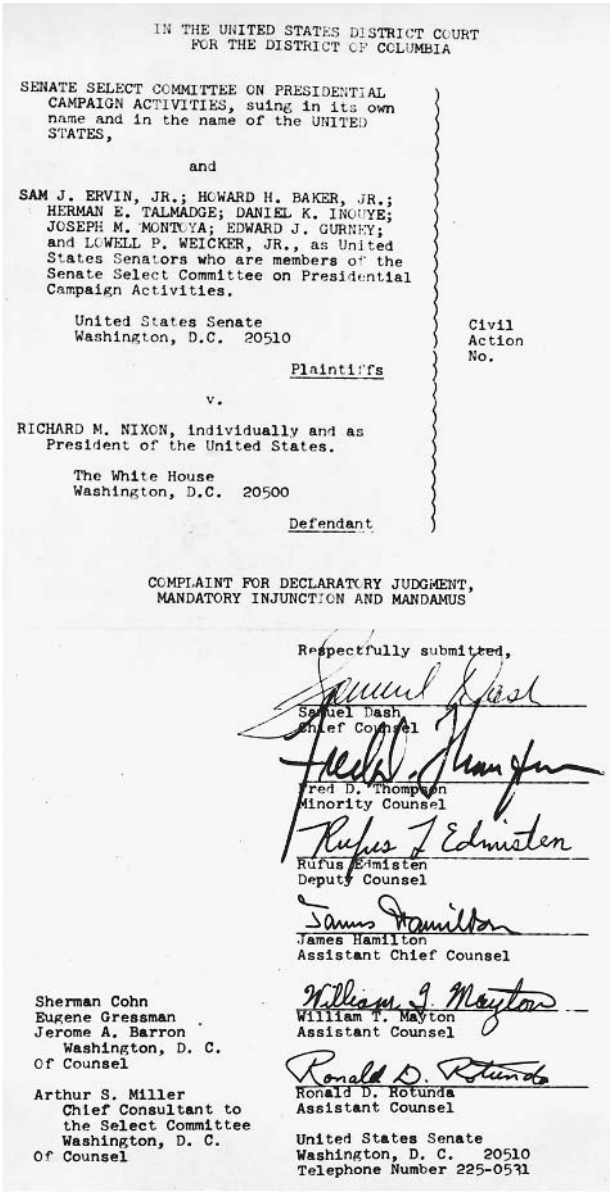
Watergate

ADRIENNE WILMOTH LERNER

Five men, known as the "White House plumbers," broke into the Watergate apartment and office complex on June 17, 1972. The well-trained burglars' mission was to raid Democratic Party offices in the complex and obtain secret documents pertaining to the presidential election. The five men, Frank Sturgis, Bernard Baker, Eugenio Martinez, Virgilio Gonzalez, and James McCord were caught and arrested. Subsequent investigations revealed the involvement of E. Howard Hunt and G. Gordon Liddy in planning the break-in, and possible connections to the White House and Central Intelligence Agency (CIA).

Three of the "White House plumbers," Liddy, McCord, and Hunt were former members of the CIA. When investigations revealed that the burglars used sophisticated eavesdropping and espionage equipment, the scandal grew to encompass the United States intelligence community. Eavesdropping devices, including wiretaps and tape recorders, were planted in the target Watergate offices before the break-in to monitor communications. During the burglary, the men used miniature cameras, complex lock picks, and military issue walkie-talkies. Authorities discovered small canisters of tear gas on two of the men. Some of the tools were even marked with government identification numbers, evidence that the operation was planned or authorized by a member of the government. The White House, and President Richard Nixon himself, were soon implicated, elevating the Watergate incident to full-fledged political scandal at the highest political level.

The men involved in the Watergate affair were members of the Committee to Re-elect the President sometimes referred to colloquially as "CREEP." Months before



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SENATE SELECT COMMITTEE ON PRESIDENTIAL CAMPAIGN ACTIVITIES, suing in its own name and in the name of the UNITED STATES,

and

SAM J. ERVIN, JR.; HOWARD H. BAKER, JR.; HERMAN E. TALMADGE; DANIEL K. INOUYE; JOSEPH M. MONTOYA; EDWARD J. GURNEY; and LOWELL P. WEICKER, JR., as United States Senators who are members of the Senate Select Committee on Presidential Campaign Activities.

United States Senate
Washington, D.C. 20510

Plaintiffs

v.

RICHARD M. NIXON, individually and as President of the United States.

The White House
Washington, D.C. 20500

Defendant

Civil Action No.

COMPLAINT FOR DECLARATORY JUDGMENT, MANDATORY INJUNCTION AND MANDAMUS

Respectfully submitted,

Samuel Dash
Chief Counsel

Fred D. Thompson
Minority Counsel

Rufus L. Edmisten
Deputy Counsel

James Hamilton
Assistant Chief Counsel

William T. Mayton
Assistant Counsel

Ronald D. Rotunda
Assistant Counsel

Sherman Cohn
Eugene Gressman
Jerome A. Barron
Washington, D. C.
Of Counsel

Arthur S. Miller
Chief Consultant to the Select Committee
Washington, D. C.
Of Counsel

United States Senate
Washington, D. C. 20510
Telephone Number 225-0571

Photo showing the first and last pages of the complaint filed in Washington, D.C., by the Senate Watergate committee in 1973 naming as defendant Richard Nixon both individually and as president of the United States. AP/WIDE WORLD PHOTOS.

the break-in, members of CREEP advised President Nixon to develop "political intelligence capabilities" to further his campaign. Facing public backlash from the war in Vietnam, Nixon's committee sought to discredit Democratic opponents in an attempt to gain ground in the election. Following the Watergate burglary, and the arrest of the "White House plumbers," Federal authorities conducted a full investigation of the incident. The White House, and CREEP, attempted to block full disclosure of the scandal.

The cover-up of the Watergate affair was itself a deft intelligence maneuver. Members of CREEP destroyed pertinent documents and encouraged allies in the United States intelligence community to do the same. The Nixon White House destroyed tape archives of phone conversations. FBI Acting Director Patrick Gray later resigned his post after admitting to destroying Watergate documents at the request of CREEP officials. Those in custody gave a series of false statements, committing perjury, in an attempt to distance the scandal from the Nixon administration. As a result, only three of the original eight men arrested were indicted. For a while, the cover-up was successful.

Following Nixon's re-election, the U.S. Senate began a formal inquiry of the Watergate scandal. The previous CIA and FBI investigations failed to implicate the Office of the President because none of the persons questioned mentioned the involvement of the White House in CREEP operations. In March 1973, Hunt asked for a significant sun of "hush money" to refrain from going to the FBI or Senate committee with information about the scandal. He received $75,000.

Most of those involved in the scandal decided to exercise their Fifth Amendment rights and not testify to the Senate committee. Nixon announced a new investigation of the scandal on March 21, 1973, but immediately began to stonewall the process. A letter from McCord to Judge Sirica on March 23 formally implicated the White House plumbers, CREEP, and the president in the Watergate scandal. The cover-up fell apart, and a desperate administration resorted to a series of "dirty tricks" to shift the focus of the investigation away from the Nixon administration.

The "dirty tricks" focused on discrediting those who testified against CREEP, White House, and intelligence agencies. Some were accused of sexual misconduct, others of financial irregularities. Stink bombs were planted in offices. However, the most devious trick was the falsification of State Department cables by Hunt to implicate former President John Kennedy in the assassination of the South Vietnamese President Diem. Hunt tried to sell the cables to the media, in an attempt to anger and influence predominantly Democratic Catholic voters. The timely surfacing of the mysterious cables, as well as public disclosure of campaign finance irregularities by the Nixon administration further fueled the scandal.

While the break-in itself was an illegal act, the Watergate scandal had far greater legal consequences. The involvement of former CIA members raised questions about the prevalence of political espionage in the United States government. Using the resources of the intelligence for political espionage or personal gain is strictly illegal under American law. In addition, the involvement of the White House implied the Office of the President resorted to gross abuses of its power and authority. Subsequent Senate hearings and FBI investigations reached similar conclusions, and nearly 30 people in the Nixon administration were fined or imprisoned.

Complex intelligence operations and sophisticated equipment had permitted the "White House plumbers," CREEP, and Nixon to perpetrate and hide many of their crimes. However, the same sophistication of cloak and dagger operations ultimately undid the Nixon administration and broke the mysteries of the Watergate scandal. Nixon recorded most conversations in his office. An intense legal battle, eventually reaching the Supreme Court, ensued over the tapes, their possible editing, and their admissibility in Senate Select Committee hearings. Facing impeachment after the subpoena of the tapes, Nixon resigned his office. Although he was later pardoned by President Gerald Ford, some of the people involved in the scandal served long prison terms, never breaking their cover story in relation to the scandal.

The most important political scandal in U.S. history was perhaps best put in perspective by the late comedian Bob Hope, who said of Watergate, "It gave dirty politics a bad name."

FURTHER READING:

BOOKS:

Bernstein, Carl, and Bob Woodward. *All the President's Men, 25th Anniversary Edition.* New York: Simon and Schuster, 1999.

Kurland, Philip B. *Watergate and the Constitution (The William R. Kenan, Jr., Inagural Lectures).* Chicago:University of Chicago Press, 1978.

Kutler, Stanley I. *The Wars of Watergate: The Last Crisis of Richard Nixon.* New York: W.W. Norton and Company, 1992.

ELECTRONIC:

United States National Archives and Records Administration. Watergate resources. <http://www.archives.gov/digital_classroom/lessons/watergate_and_constitution/teaching_activities.html>(01 December 2002).

SEE ALSO

Church Committee
Vietnam War

Weapon-Grade Plutonium and Uranium, Tracking

K. LEE LERNER/LARRY GILMAN

Weapon-grade (or "bomb-grade") uranium or plutonium is any alloy or oxide compound that contains enough of certain isotopes of these elements to serve as the active ingredient in a nuclear weapon. Some civilian weapon-grade materials are tracked by international organizations, especially the United Nations' International Atomic Energy Agency (IAEA) and the European Atomic Energy Community (EURATOM), to prevent their diversion to bombs. The goal is to prevent nuclear proliferation, that is, the possession of nuclear weapons by more and more groups.

IAEA safeguards track weapon-grade materials (or, in the case of plutonium, dilute materials that could be refined to weapons grade) in non-military nuclear fuel cycles in states that are signatories to the Non-Proliferation Treaty (NPT) of 1968. Those states that already had nuclear weapons at the time of the treaty's creation—the U.S., United Kingdom, France, Russia, and China—are not subject to IAEA safeguards. Only four states—Cuba, India, Israel, and Pakistan—have not signed the NPT and are not part of any international safeguard system. Of these four, all have nuclear weapons except Cuba, which western intelligence agencies assert is not currently seeking nuclear weapons. EURATOM safeguards civil plutonium and uranium in the European countries, including materials not covered by mandatory IAEA safeguards under the NPT (i.e., those in the UK and France). The IAEA and EURATOM cooperatively safeguard European materials to avoid redundancy.

Military nuclear materials are tracked not by the IAEA but by the governments that own them. Because the tracking techniques employed internally by nuclear-weapons states vary from nation to nation and are always partly or wholly secret, and since EURATOM safeguards are essentially the same as IAEA safeguards, this article restricts itself to IAEA safeguards on nuclear materials in the 182 non-nuclear-weapons signatories of the NPT.

Definition of "Weapon-Grade"

"Weapon-grade" uranium or plutonium is sometimes defined as any alloys pure enough to be used in bombs by governments building light-weight nuclear weapons for carriage in missiles, artillery shells, or other delivery systems. The highly-enriched uranium (HEU) preferred by professional weapons designers is more than 90% uranium-235 (^{235}U), and the enriched plutonium used for such purposes is nearly pure metal. However, "weapon-grade" it is more usefully, and more commonly, defined as any material pure enough to serve in a nuclear weapon, regardless of that weapon's efficiency or elegance of design. Uranium enriched to only about 50% ^{235}U, and probably less, can be used to make a crude nuclear bomb, and it is possible to make a bomb from material that is only 15–25% plutonium (e.g., mixed-oxide fast breeder reactor fuel). A "crude" bomb would probably have an explosive force of several tens of kilotons (where one kiloton equals the explosive force of one thousand tons of trinitrotoluene, TNT), comparable to the bombs that destroyed Hiroshima and Nagasaki in 1945.

Weapon-grade fissile materials are not found in nature, but must be produced. ^{235}U is found only in dilute form in nature. It constitutes about .71% of the uranium in ore, the rest being mostly the isotope ^{238}U, which is not fissile enough to be a reactor fuel or bomb material. Reactor-grade uranium (i.e., the fuel for civilian nuclear power plants, which is about 3% ^{235}U) and weapon-grade uranium are obtained by enriching the concentration of ^{235}U in metal extracted from ore, a complex and expensive industrial process. The nearly pure ^{238}U that is left over from enrichment, although useless as a fuel or explosive, can be partly transformed into plutonium by neutron bombardment in a particle accelerator or nuclear reactor. (There are several isotopes of plutonium, not all equally suitable for bombs, but because all readily available isotopic blends of plutonium are suitable for bomb-making, this article refers simply to "plutonium.")

These facts are important to the tracking or safeguarding of weapon-grade material. Since ^{235}U exists in nature and only needs to be concentrated to become a bomb material, an ideal tracking system for would station observers at every stage of uranium extraction and refinement, from the mine to the enrichment plant. This would cost too much, so the IAEA monitors selected industrial processes, namely enrichment plants, fuel-fabrication facilities, and reprocessing facilities. A reprocessing facility is a factory where nuclear-reactor fuel that has been isotopically altered by irradiation in a reactor core and is no longer isotopically optimal for fuel purposes ("spent" fuel) is dissolved in acid and its ^{235}U and plutonium separated out. (What is left is high-level nuclear waste.) Reprocessing is the sole source of weapon-grade plutonium, as plutonium occurs in nature only in trace amounts; therefore, IAEA safeguards track not only separated plutonium but spent nuclear fuel.

The Safeguarding Task

There are three basic stocks or inventories of weapon-grade (or pre-weapon-grade) material: military inventories, transitional inventories, and civil inventories. *Military inventories* consist of fissile materials (almost entirely alloys of uranium and plutonium) that are already built into weapons, are stockpiled for possible weapons use, or are stockpiled for or already used in naval reactors. (Due to size constraints, the reactors used to drive some submarines and military surface ships require weapon-grade

uranium as fuel). *Transitional inventories* consist of materials that have been removed from weapons or declared by the states that own them to be in excess of their weapon-making needs. By far the largest transitional stockpile in the world is that of Russia, nuclear inheritor state of the Soviet Union. *Civil inventories* consist of materials belonging to the nuclear-power fuel cycle, including stockpiled HEU and plutonium separated from spent fuel, plutonium and HEU loaded or stockpiled as fuel for specialized reactors (e.g., fast breeders), and plutonium and HEU in spent reactor fuel of all types. The basic goal of international safeguards is to track materials in the transitional and civil inventories to prevent them from being secretly diverted to weapons by terrorists or governments. (Although the transitional inventories are held by nuclear-weapons states not required by the NPT to submit them to IAEA safeguards, some of them, notably Russia's, are voluntarily submitted to IAEA safeguards.)

About 3,000 tons of plutonium and HEU have been produced by the civil and nuclear military facilities to date, with hundreds of kilograms of new plutonium forming constantly in the fuel rods of nuclear reactors worldwide. About 700 of these tons are in military inventories, about 1,300 tons in transitional inventories (mostly in the U.S. and Russia), and about 1,000 tons in civil inventories. Because the civil inventories in some of the largest nuclear-power states (i.e., the U.S., U.K., France, and Russia) are not subject to IAEA safeguards, only about 24 tons of weapon-grade plutonium and uranium—less than 1% of the world stock of these materials—is safeguarded. Though apparently small, this quantity of material could produce hundreds of nuclear weapons, and is exactly that fraction of the world's HEU and plutonium inventory that is most vulnerable to diversion. The IAEA, like a border patrol, thus deploys its forces along a critical edge rather than spreading them over the domain of all weapons-grade materials.

Safeguards are designed to deter—by making it difficult to conceal—any attempt to concentrate non-weapon-grade nuclear material into weapon-grade material or, alternatively, to divert weapon-grade material from peaceful purposes (e.g., breeder-reactor fuel) to weapons. Safeguards are thus after-the-fact measures designed to detect a material diversion that has already occurred, quickly enough to detect the diversion before a nuclear weapon can be assembled.

Methods

The two basic methods used to track weapons-grade nuclear material are accountancy and physical inspection.

Accountancy. The NPT requires every signatory nation to "establish and maintain [its own] system of accounting for all nuclear material subject to safeguards," that is, HEU and plutonium. In other words, the IAEA seeks to build on national accounting controls rather than building its own system from scratch. (It does so not because national controls are intrinsically better, but to control costs.) The IAEA specifies, in part, what these national accounting procedures shall be, in order to assure that their adequacy and compatibility with the IAEA's own methods.

In this context, a "system of accounting" means a system of inventorying, similar in principle to that used to run a grocery store. The IAEA defines "material balance areas," specific physical zones which may be as large as entire facility or as small as a single room, for which inventories must be kept. Whenever safeguarded materials are brought in or out of a material balance area, records must be made of the amounts, entering, leaving, and in the material balance area. If the totals do not add up, a diversion is suspected.

Inspection. The fact that a nation is responsible for inventorying its own nuclear materials creates an obvious opportunity for cheating: a state might simply fabricate records that show no diversions. To prevent this, the IAEA analyzes each nation's records for inconsistency or other signs of fraud. More importantly, it conducts on-site inspections. Formerly, inspection consisted mostly of visits by IAEA personnel. Site visits by inspectors remain essential, but with the development of new detection technologies and computer systems, automatic or "unattended" safeguards have become more widely used. For example, all entry points to a material balance area might be recorded continually on sealed videotapes that are later analyzed by the IAEA for suspicious activity. Sensors that detect the presence, type, and quantity of nuclear materials by measuring neutrons, alpha particles, or gamma rays can be located at the access gate of a reprocessing plant, near a fuel-storage area, or in other key locations. (Inspections or video monitoring would assure that temporary exits are not being cut in the perimeter fence elsewhere, to escape surveillance.) The efficacy of inspection is increased by requiring that the NPT signatory state whose materials are being safeguarded submit information about the design of its nuclear facilities to the IAEA. The IAEA may also place special seals on containers of safeguarded material, then re-inspect periodically to verify that the seal has not been broken, and require that an inspector be present if the seal is to be broken. The purpose of inspections is, in short, not to directly track all flows of safeguarded material, but to keep the inventory system honest.

Measurement inaccuracy. All the measurement processes involved in tracking HEU and plutonium have built-in error. If, for example, a particular scale is only accurate to within a milligram, then there is always 1 mg of uncertainty about how much HEU or plutonium is resting on it. If

a sample of HEU or plutonium that is known to have a mass of 1.00 g is broken in two and each piece measured on a scale having 1-mg inaccuracy, and if these two measurements both read .499 g (for a total of .998 g), it is impossible to tell whether .002 g of controlled material has been diverted or the numbers merely reflect random measurement error. To combat this source of uncertainty it is possible to screen for "systematic" errors, that is, errors that trend systematically in some direction; in particular, errors that always show a loss of material rather than a gain would be more suspicious. (Truly random error should sometimes show too much, rather than too little, material.) However, clever manipulation of error margins inside a complicated system could pit false gains against real losses, thus preventing the appearance of systematic error and concealing small, persistent diversions.

In reprocessing facilities, which extract HEU and plutonium from spent fuel, this problem is particularly acute, as a material balance can only be performed on each batch of liquid material processed by the plant. Cumulative material-balance inaccuracies of up to 1% are probably unavoidable in reprocessing. In a reprocessing facility such as the U.K.'s Barnwell, which was originally designed to extract 15 tons of plutonium per year from 1500 tons of spent fuel, this would mean that 150 kg of plutonium could be diverted undetectably from the plant every year—enough for about 15 atomic bombs. The IAEA Safeguards Division seeks to track inventories in individual states to within 8 kg of plutonium and 25 kg of HEU annually—enough to easily build a single bomb. However, if a state was willing to wait a few years for each bomb, its diversions could remain within the intrinsic error limits.

Strengthened safeguards. In the early 1990s, IAEA inspectors discovered that Iraq, though a signatory of the NPT and subject to the full range of IAEA safeguards, had for years been conducting a covert nuclear-weapons program involving thousands of personnel, mostly at facilities already subject to IAEA inspection. It was the first serious attempt by an NPT signatory state to circumvent IAEA safeguards, and was partly successful. Judged by its ultimate goal, however—to produce nuclear weapons—it was an apparent failure; given information by U.S. and U.K. intelligence agencies, IAEA inspectors finally became suspicious and detected the fraud. IAEA inspectors asserted that Iraq (prior to the 2003 American-led war to disarm Iraq) had not been able to reconstitute its nuclear weapons program. In any case, the incident proved that existing IAEA safeguard standards were inadequate. These have been replaced by what the IAEA terms the "strengthened international safeguards system," which includes stricter and more thorough inventorying; greater access to information about reactor-facility designs, uranium mines, and uranium concentration plants; environmental sampling for signs of radioactivity; more complete facility access; and surprise inspections.

FURTHER READING:

BOOKS:

Arlt, R., et al. "Use of CdZnTe Detectors in Hand-Held and Portable Isotope Identifiers to Detect Illicit Trafficking of Nuclear Material and Radioactive Sources." Nuclear Science Symposium Conference Record, Vol. 1, IEEE, 2001: 4–18; 4–23.

Koster, J. E., et al. "Alpha Detection as a Probe for Counter Proliferation." 28th Annual International Carnahan Conference on Security Technology, 12–14 Oct. 1994, IEEE, 1994: 6–19.

Lovett, James E. *Nuclear Materials: Accountability Management Safeguards.* American Nuclear Society, 1974.

Mercier, M. T., R. J. Huckins, and G. S. Zalokar. "A Local Data Acquisition Subsystem for Plutonium Safeguards." Nuclear Science Symposium and Medical Imaging Conference Record, 2–9 Nov. 1996, IEEE, 1996: 1254–59.

Walker, William, and Frans Berkhout. *Fissile Material Stocks: Characteristics, Measures and Policy Options.* New York: United Nations, 1999.

Willrich, Mason, ed. *International Safeguards and Nuclear Industry.* Baltimore, MD: Johns Hopkins Press, 1973.

ELECTRONIC:

International Atomic Energy Agency (IAEA). 2003. <http://www.iaea.org/worldatom/> (April 2, 2003).

Lu, Ming-Shih. "The IAEA Strengthened International Safeguards System." Brookhaven National Laboratory. 1998. <http://www.nautilus.org/library/security/papers/LuISODARCO.PDF> (April 2, 2003).

Weapons of Mass Destruction

ALEXANDR IOFFE

The concept of Weapons of Mass Destruction appeared during War World II after the use of atomic bombs. In the mass consciousness, weapons of mass destruction are usually associated first with atomic weapons, although the concept includes certain chemical and biological weapons.

The atomic bomb was used only twice in World War II, in bombarding the Japanese cities of Hiroshima (August 6, 1945) and Nagasaki (August 9, 1945) by the United States. The first bomb employed uranium-235 and produced an explosion equivalent in power to approximately 15 kilotons of TNT gunpowder. The second bomb employed plutonium and was equivalent in power to approximately 21 kilotons of TNT gunpowder.

On August 7, 1945 the General Staff of Japan received an alarming telegram from the Hiroshima region claiming that the city was completely destroyed by one bomb. Approximately 130 thousand people were killed because of the bombardments of both cities, and both Hiroshima and Nagasaki were completely destroyed. The number of

injured also numbered in the hundreds of thousands, and the consequences of burns and radiation were apparent in bombardment victims for many years, often including the next generation.

The process of radioactive isotope (uranium-235 or plutonium-239) fission is the basis of the action of atomic weapons. A mammoth amount of energy is generated in this process. The dissipation of energy in an atomic bomb explosion occurs in the following approximate ratio: bomb blast and wind – 50%; thermal rays – 35%; and (radioactive) radiation – 15%. These are the three main striking factors of an atomic explosion.

An even more powerful weapon, the hydrogen fusion bomb, was created several years after the A-bomb, and was created practically simultaneously in USA and in the former Soviet Union. The power of the H-bomb is hundreds of times higher than the power of an A-bomb. The process of hydrogen isotope fusion is the basis of the thermonuclear weapon action. The start of this reaction, however, must be initiated by a nuclear fission explosion.

On November 1, 1952, a 10.4 megaton thermonuclear explosion code-named MIKE, ushered in the thermonuclear age (it was an explosion of a special model of the device). The island of Elugelab in the Eniwetok Atoll in Pacific was completely vaporized.

The first H-bomb was exploded in the USSR in August, 1953, followed on March, 1, 1954, by the American explosion of a more powerful hydrogen bomb (approximately 15 megatons). The Soviets responded with the most powerful H-bomb explosion yet, in the Soviet Union on October 15, 1961, over the Novaya Zemlya (New Earth) island (in the Polar Ocean) at a height of 4000 meters (approximately. 13,000 feet) over the Earth. Its power was almost 50 megatons. A gigantic fireball was created by the explosion that reached to the height of about 67 km (41.5 miles), and its light was seen for a distance of more then 1000 km (621 miles). The explosion also resulted in a blast of wind that was felt for hundreds of kilometers.

The creation of the atomic bomb in the USA during World War II was an exceptional scientific phenomenon. The interval between the discovery of the physical fusion process that is the basis of the weapon action, and the moment of its first test (July 16, 1945, in the New Mexico desert) was only several years, and up to the end of this test, its creators were not absolutely sure that the test would be successful. The United States committed an enormous amount of scientific and monetary resources towards the creation of the atom bomb, and a new branch of industry was formed.

In 1949, the A-bomb was also created in the USSR. Later, a big concern among American intelligence authorities arose about atomic espionage, which helped the Russians to create the A-bomb during such a short period. Several people who passed to the Russians secrets about atomic elaboration were revealed and arrested, including Claus Fuchs and Julius and Ethel Rosenberg. Although some thought that espionage was the crucial factor in the Russian's success, the main secret was whether the nuclear chain reaction of the A-bomb could be successfully created and controlled. As soon as the bomb exploded over Japan, this secret became clear. Additionally, in 1945, a noted report by American physicist H. D. Smith entitled *"Atomic Energy for Military Purposes"* was openly published, in which the principles of the bomb's action, the methods of isotope separation, and even some of the characteristics of its construction were described in detail. The post-war Soviet Union of 1945 still contained highly qualified scientists, and the totalitarian regime dedicated all possible resources to the high-priority project of atomic bomb development. Thus, the arms race of the 1960s and 1970s has its beginnings as far back as the early post–World War II era.

Many chemical weapons are also considered weapons of mass destruction. Various lethal poisons were known and successfully used in warfare as long ago as ancient times. The creation of such substances for weaponry is much easier and cheaper than, for example, separating uranium isotopes as is necessary for a nuclear weapon. Chlorine gas, for example, one of the simplest poison gases, can be created in small amounts in a simple laboratory. The problem of delivering poison gases to a battlefield is also much simpler than delivering an atomic weapon.

During World War I, the Germans were the first to use poison gases on the modern battlefield. The Germans bombarded their enemies with artillery shells armed with poison gas, or simply ejected gas from their containers. The names of some poison compounds are reminiscent of World War I; for instance, the poison gas yperite (mustard gas) has in its origin the name of the Belgian city Yper, where the gas was used the first time. In 1915, the Germans also conducted massive attacks using chlorine. As a result of one chlorine gas attack, five thousand persons were killed and about ten thousand were injured. The Germans ejected chlorine from 5730 balloons containing about 168 tons of chlorine within the 5 to 8 minute duration of the attack.

Officially, the use of chemical weapons is forbidden by the Hague Conventions concluded in 1899 and 1907, and these resolutions were further clarified and strengthened by the Geneva Protocol of 1925. The first international disarmament treaty that banned the production and stockpiling of biological weapons, and provided for destruction of existing stores became open for signature in 1975. Almost 30 years later, the treaty is still the subject of regular debate and clarification and lacks wide spread ratification.

In the meantime, chemists of various governments have worked actively to create new chemical substances with various destructive factors. Additional chemical weapons have been derived from toxic industrial chemicals that were originally designated for useful purposes, such as pesticides. Chemical weapons can generally be divided among several groups, depending on their action on people, including vesicants, toxins, incapacitating agents, nerve

agents, and irritants. The production of vesicants is not technologically complicated. The production of the nerve agents, however, requires significantly more sophisticated chemical processing. Some production processes require strict temperature control, and containment of the toxic substances and gases can pose problems. Depending on the immediacy of use, purity of the product can add a difficult dimension to production. In some cases, special equipment or handling is required to prevent corrosion of equipment and/or rapid deterioration of the product.

Chemical weapons were not used during World War II, although the main participants had large reserves of such weapons. Production of these weapons continued after World War II, and only recently the USA and Russia have stopped their production and agreed to begin to destroy existing stockpiles. Other nations and extremist groups have recently used chemical weapons. Iraq used chemical weapons during the Iran-Iraq war (probably a somewhat over-fluorinated DC, methylphosphonic dichloride) during the 1980s. Iraq additionally used Sarin gas on its own Kurdish population, killing thousands of citizens in the town of Halabja in 1988. Sarin gas was also the weapon used in an attack on the subway in Tokyo in 1995 by the Japanese extremist religious sect Aum Shinrikyo, in which 17 persons were killed and hundreds were injured.

Biological weapons are also capable of mass human destruction. The basic action of a biological weapon involves the use of pathogenic (disease-causing) bacteria, viruses, fungi, or toxins produced by some bacteria. Biological weapons contain particular dangers because they can provoke perilous diseases in people and animals over large geographic areas, as the effectiveness of the weapon multiplies with the spreading of communicable disease. The destructive period can be lengthy with the use of a biological weapon, and it can have latent (incubation) period of action.

What makes biological weapons so dangerous are that the cost to produce such weapons is nominal as compared to the cost to make nuclear weapons. This is why biological weapons are often considered as the terrorist or poor nation's weapon of mass destruction. Also, the production of biological weapons can be easily hidden, as there are no special factories or highly specialized equipment needed for their production. Biological weapons can be deployed silently, through crude crop dusters, the mail, or even bug bombs, therefore allowing for the initial escape of their deployers. Unlike their counterparts (chemical and nuclear weaponry), biological weaponry products are living organisms and do not break down overtime, but in-fact can multiply and increase in numbers.

There is a long list of BW agents that could potentially be used in a war or a terrorist attack. Among those mentioned have been anthrax, cryptococcosis, *Yersina pestis* (plague, the Black Death of the 14th Century), tularemia (rabbit fever), malaria, cholera, typhoid, smallpox, cobra venom, and others. Some authors have also speculated about the possible terrorist use of new, genetically engineered agents designed to defeat conventional methods of treatment, or to attack specific peoples.

The idea of using biological agents in war is not new. In the 6th century B.C., Solon of Athens used the purgative herb hellebore (skunk cabbage) to poison the water supply during the siege of Krissa. In 1346, plague broke out in the Tartar army during its siege of Kaffa (at present day Feodosiys in the Crimea), after attackers hurled the corpses of those who died over the city walls. The plague epidemic that followed forced the defenders to surrender, and some infected people who left Kaffa may have started the Black Death pandemic that later spread throughout Europe. In 1797, Napoleon attempted to infect the inhabitants of the besieged city of Mantua with swamp fever during his Italian campaign. An attempted biological attack was undertaken in 1915 by the German-American physician Dr. Anton Dilger (in Baltimore) who attempted to infect a reported 3000 head of horses, mules, and cattle destined for the Allied forces in Europe. Nowadays, the specter of annihilation by killer pathogens or toxins has, in some sense, replaced the Cold War nightmare of extermination by massive nuclear attack.

Since 1972, the use of biological weapons is prohibited by the international treaty, as reflected in its formal title, the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction. As of 2003, the agreement had 144 nation-state signatories.

FURTHER READING:

BOOKS:

Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction.* Washington, DC: Carnegie Endowment for International Peace, 2002.

Hamzah, Khidr Ald Al-Abbis, and Jeff Stein. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraq Nuclear and Biological Weapons Agenda.* New York: Scribner, 2002.

Harris, Robert, and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare.* New York: Random House, 2002.

Lavoy, Peter R., Scott D. Sagan, James J. Wirtz. *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons.* Cornell: Cornell University Press, 2001.

Rhodes, Richard. *Dark Sun: The Making of the Hydrogen Bomb (Sloan Technology Series).* Simon & Schuster, 1995.

Roberts, Brad. *Biological Weapons: Weapons of the Future?* Washington, D.C.: Center for Strategic and International Studies, 1993.

Sagan, Scott D. and Kenneth N. Waltz. *The Spread of Nuclear Weapons: A Debate Renewed,* Second Edition. W W Norton & Co., 2003.

Walmer, Max. *An Illustrated Guide to Strategic Weapons.* New York: Prentice Hall Press, 1998.

PERIODICALS:

DaSilva, E., "Biological Warfare, Terrorism, and the Biological Toxin Weapons Convention." *Electronic Journal of Biotechnology* 3(1999):1–17.

Dire, D.J., and T.W. McGovern. "CBRNE—Biological Warfare Agents." *eMedicine Journal,* 4 (2002):1–39.

Macintrye, A. G., C. G. W. Eitzen, Jr., and R. Gum, et al. "Weapons of Mass Destruction Events with Contaminated Casualties: Effective Planning for Health Care Facilities." *Journal of the American Medical Association* no. 283 (2000): 252–253.

Munro, N.B., S.S. Talmage, G.D. Griffin, et al. "The Sources, Fate, and Toxicity of Chemical Warfare Agent Degradation Products." *Environmental Health Perspectives* no. 107 (1999): 933–974.

Nakajima, T., S. Ohta, Y. Fukushima, et al. "Sequelae of Sarin Toxicity at One and Three Years after Exposure in Matsumoto, Japan." *Journal of Epidemiology* no. 9 (1999): 337–343.

ELECTRONIC:

How Stuff Works. "How Biological and Chemical Warfare Works." 2002. <http://www.howstuffworks.com/Biochem-war.htm>(10 January 2003).

United States Department of State. "Parties and Signatories of the Biological Weapons Convention." December 11, 2002. <http://www.state.gov/t/ac/bw/fs/2002/8026.htm> (February 25, 2003).

SEE ALSO

Anthrax, Terrorist Use as a Biological Weapon
Anthrax Vaccine
Anthrax Weaponization
Arms Control, United States Bureau
Biological Warfare
Biological Warfare, Advanced diagnostics
Biological Weapons, Genetic Identification
Bioterrorism, Protective Measures
Chemical Warfare
Manhattan Project
North Korean Nuclear Weapons Programs
Nuclear Detection Devices
Russian Nuclear Materials, Security Issues
Tabun
USAMRIID (United States Army Medical Research Institute of Infectious Diseases
Vozrozhdeniye Island, Soviet and Russian Biochemical Facility
World War I
World War II

Weapons of Mass Destruction, Detection

K. LEE LERNER/BRIAN HOYLE

Weapons of mass destruction are weapons that cause a high loss of life within a short time span. Nuclear, chemical, and biological weapons fit this definition.

An atomic bomb exploded over a densely populated city could kill hundreds of thousands of people instantaneously and, as the lethal effects of radiation exposure take hold, causes many more deaths within days or weeks. Chemicals such as Ricin that disrupt nerve function are lethal upon exposure. Agents such as mustard gas can cause life-threatening burns. Chemical weapons can affect a wide geographical area because the chemicals are dispersed in the air.

Biological weapons take longer than nuclear and chemical weapons to cause damage. Because infections can subsequently spread through a population far from the site of contamination, and because the population may not be protected by vaccination or natural immunity to the microorganism responsible for the infection, the eventual death toll from an organized biological attack, however, could reach into the millions. Relevant modern day examples of biological weapons of mass destruction are anthrax (caused by *Bacillus anthracis*), plague (caused by *Yersinia pestis*), and smallpox (caused by the variola virus).

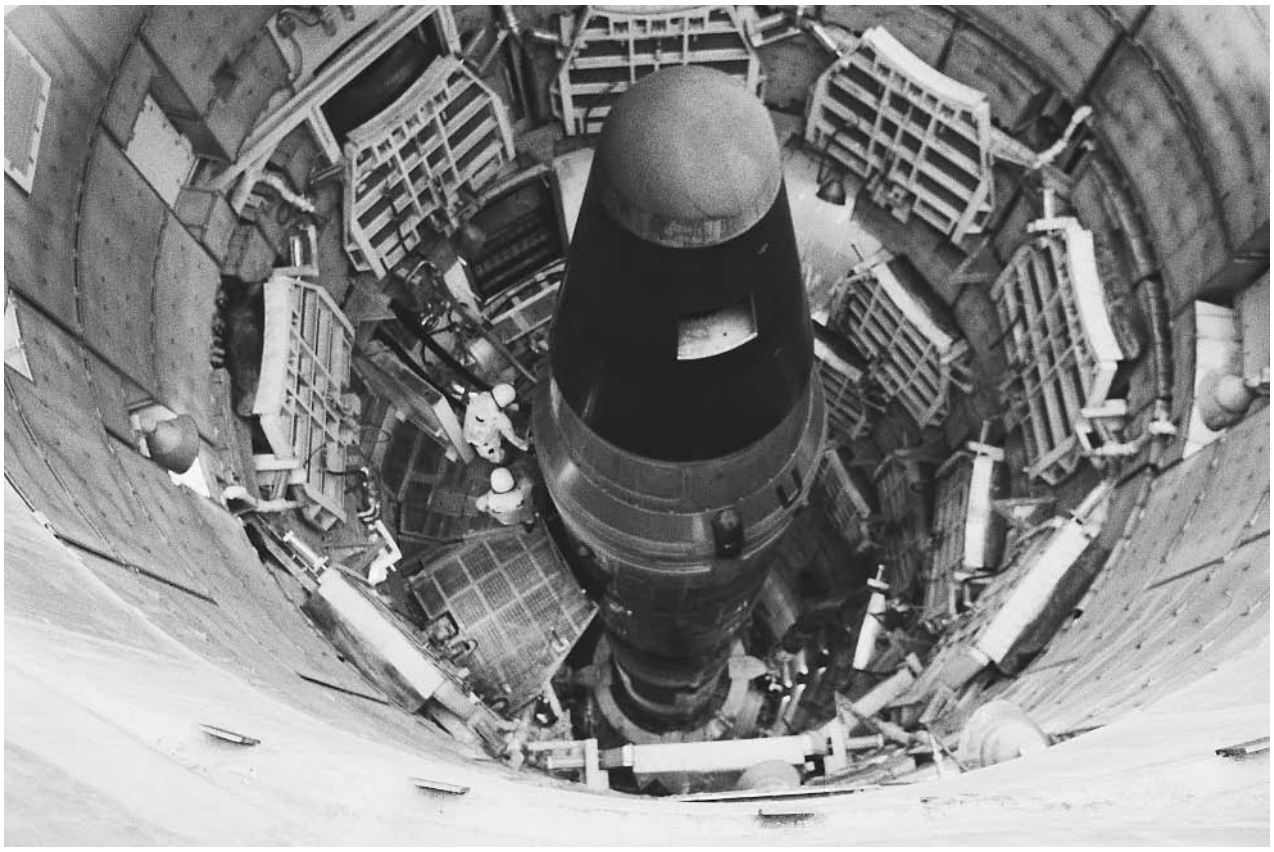
The damage from weapons that are less powerful or toxic can be minimized. For example, buildings can be fortified to withstand assaults from conventional explosives such as grenades. Thus, for such weapons, damage prevention can be the priority rather than detection. However, the damage from a weapon of mass destruction cannot be minimized once the weapon has been unleashed. Rather, the weapons need to be detected before they are used.

Detection of Chemical and Nuclear Weapons of Mass Destruction

Chemical and nuclear weapons are often delivered to their target in missiles. Sophisticated open-air launch facilities and large pieces of equipment are required for launch, and it is difficult to conceal such facilities from aerial surveillance. Planes, unmanned drones, and even satellites positioned over a region will all reveal the presence of a missile installation. Underground chemical storage facilities can also be revealed by the use of ground penetrating radar.

The materials that are commonly used in the construction of chemical and nuclear weapons can be detected. For example, an instrument called the Dual-Use Analyzer uses the phenomenon of eddy current. An electrical current is passed through a sample, and the conductivity of the metal produces a characteristic signal. If another metal is present, such as those used in chemical and nuclear weapons, another signal is produced. The rogue signal can be compared to a databank of signals produced by metals that are typically used in weapons.

Light or radiation. The airborne release of chemical weapons can be detected using light. Specifically, the scattering or absorption of a directed beam of laser light, or



Interior of an intercontinental ballistic missile silo. ©STEVE JAY CRISE/CORBIS.

the development of fluorescence when the aerosol cloud contacts laser or ultraviolet light, can detect a chemical cloud at a distance. This sort of detection is not specific. The identity of the compound in the aerosol cloud cannot be determined. But detection can provide some time for preparations (i.e., evacuation gathering in an airtight facility). Specific detection methods, however, are possible. Chemical groups behave in distinctive ways when exposed to different kinds of light or radiation. The measurement of the chemical behavior is called spectroscopy. The machines that perform the analysis are called spectrometers.

In mass spectroscopy, the mass (or molecular weight) of proteins is determined. The molecular weight is an important means of identifying a protein. In turn, the identification of a protein can provide a clue as to what chemical agent is present. Raman spectroscopy relies on the change in the shape and frequency of the wave of light (i.e., the wavelength) as it passes through a sample to identify the chemical groups that cause the wavelength change. In neutron spectroscopy, neutrons interact with the chemical groups of the sample. The patterns of these interactions can be measured and used to identify chemical groups. Neutron spectroscopy is especially adept at detecting plutonium, and thus is useful in the detection of nuclear weapons. Finally, optical spectroscopy relies on the use of ultraviolet and infrared light. The absorption of the light energy by sample chemical groups, and the giving off of light of a different wavelength by the groups, is used to identify compounds, particularly compounds present in certain explosives.

A Geiger counter is a traditional portable radiation detection device. Here, a tube of gas becomes charged when neutrons pass through the tube. The charged particles are converted to an electrical signal that produces a read-out of the intensity of the radiation.

The U.S. Department of Energy's Argonne National Laboratory has developed a portable device that can detect nuclear weapons. The heart of the device is a small wafer made of gallium arsenide—a material that is similar to silicon—that is coated with boron or lithium. The coated wafer can detect neutrons that are given off by radioactive sources like plutonium^{239} and uranium ^{233}. Another portable sensor detects alloys like zirconium, which are typically used in nuclear weapons. The United Nations (U.N.) weapons inspectors in Iraq utilized this sensing technology during inspections in 2003.

Sound. Sandi National Laboratories in Albuquerque New Mexico has developed a portable machine that can detect and identify 18 different chemicals in a vapor within a few

minutes. This enables an on-the-spot detection of chemicals, which is applicable to the battlefield or to the detection of a planted chemical weapon. The compounds that can be detected can be present in chemical, nuclear, and biological weapons.

The basis of the detection is the acoustic wave sensor. A quartz surface can detect an electric signal and convert it to an acoustic signal. The acoustic signal then radiates over the quartz surface as a wave. As the wave moves, it encounters a film of material that has been coated onto the quartz. The chemical nature of the coatings determines what acoustic signal will register. The film slows down the speed of the acoustic wave, which can be used to identify the source of the wave.

The technique of acoustic resonance can reveal whether the interior of a missile is solid or whether it houses a liquid. The distinction is based on the resonance, or vibration, from inside a shell as the shell is vibrated by sound waves. Because different chemicals resonate at different frequencies of sound, the technique can even be used to determine the type of chemical housed in the shell. The device was first used by U.N. inspectors in Iraq in 1997.

Chemical reactions. Detection of chemical weapons can be accomplished by several methods. One means is by the use of detection paper. Dyes and pH indicator (an indicator of the concentration of hydrogen or hydronium ions in a solution) are incorporated into a cellulose paper. When a drop of liquid that contains a chemical warfare agent is spotted onto the paper, one of the indicators is dissolved (the particular indicator being dependent on the chemical agent present). The result is a color change. For example, mustard agent dissolves a red dye, and nerve agent dissolves a yellow dye. Other compounds like fat, oil, and fuel can also dissolve the dyes, which produces a false positive reaction. But, with careful use of the paper, the presence of chemical warfare agents can be detected.

Mustard gas can also be detected by sucking air through a tube containing an indicator compound. A reaction between the compounds produces a blue color when the tube is heated.

Detection of Biological Weapons of Mass Destruction

The identification of proteins by mass spectroscopy can be an efficient and rapid way to identify bacteria. An example is Matrix-Assisted Laser Desorption/Ionization Mass Spectroscopy (MALDI-MS). MALDI-MS can separate and detect different proteins in less than one second. The pattern that is produced is analyzed and the areas of the pattern that are unique to bacteria such as *Bacillus anthracis* (the cause of anthrax) and *Yersinia pestis* (the cause of plague) are identified.

Genetic technologies. The genetic detection of biological agents has become exquisitely sensitive. Gene probe sensors can detect and identify bacteria based upon the presence of a stretch of genetic material that is unique to the microorganism. An example is the use of the gene probe technology of the polymerase chain reaction (PCR). PCR detects a pre-determined sequence of genetic material and then produces copies of the target region. Millions of copies can be produced within a hour, allowing the sequence to be detected and studied using other tests (i.e., gel electrophoresis).

When PCR was first introduced, the equipment required dedicated space in a lab. Now, however, the equipment has been miniaturized so that it can fit into a standard briefcase. For example, the Lawrence Livermore Laboratory has developed the Handheld Advanced Nucleic Acid Analyzer (HANAA). The HANAA is about the size of a brick. The genetic probes that are used are designed to detect specific microorganisms. The microbes of interest are *Bacillus anthracis* and *Yersinia pestis*. The unit is being used in the 2003 inspection of Iraqi facilities by U.N. officials, an inspection that is designed to verify Iraqi's submitted list of biological weapons, and to reveal any expansion of the nation's biological warfare program since the Gulf War of the mid 1990s.

In contrast to the handheld detector, which operates periodically and under human control, the Autonomous Pathogen Detection System (APDS) is designed to operate continuously and without operator assistance. A fan pulls in air, and any biological material is used for PCR analysis. The APDS, which is about the size of a mailbox, is positioned where round the clock monitoring is critical. The unit can be programmed to sound an alarm when a chemical unique to bacterial spores (including anthrax spores) is present. As well another reaction causes the development of fluorescence. The intensity of the fluorescence is related to the number of spores present.

In 2002, the PCR technology was successfully adapted to allow the detection of the smallpox virus within a few minutes. As of 2003, the rapid test for smallpox is still being refined in the laboratory. However, it will doubtless not be long before the smallpox test is portable enough for use in the field.

Microorganisms can also be rapidly detected using antibodies that have been produced to certain components of the organisms. The binding of the antibody to the corresponding antigen can identify *Bacillus anthracis* in 15 minutes, for example. The same technology can be used with antibodies to other bacteria (e.g., *Clostridium botulinum* and viruses (e.g., smallpox), as well as to chemicals such as ricin.

Electrophoresis and chromatography. If a sample is suspected of containing a biological threat, the genetic material (deoxyribonucleic acid; DNA) present in the sample solution can be extracted from the other materials and analyzed. The analysis involves cutting the DNA into a variety

of pieces using enzymes that recognize specific sequences of nucleotides (the building blocks of the DNA). When the pieces of DNA are electrophoresed a series of bands results in the electrophoretic gel. The pattern of the bands is compared to patterns in a database. If an exact match is found, then the identify of the microorganism is established.

The various types of chromatography all distinguish different chemical groups from one another by the varying behaviors of the groups in certain environments. For example, one chemical group may move more slowly through a certain liquid than another chemical group. Thus, the two groups can be separated from one another. Furthermore, the pattern of their movements provides a fingerprint to identify the chemical natures of the compounds.

Microorganisms can be detected by a technique called gas liquid chromatography. The method detects fatty acids, which are a portion of the lipid molecules that make up the membrane(s) that surround microorganisms. This type of detection still requires a bulky machine and the use of specialized personnel. Nonetheless, if the need for detection is on the order of days rather than minutes, then fatty acid analysis is a useful and accurate technique.

Filters. Microorganisms like bacteria and fungi that are floating in the air can be detected by sucking the air through a filter. The filter traps the microorganisms. The filter is then placed in contact with a food source that encourages the growth and division of the bacterial or fungal cells. Within about 24 to 48 hours the microorganisms have grown and reproduced enough to form a visible clump of cells called a colony. This technology is also portable.

Detection of Weapons of Mass Destruction in Iraq

In November 2002, a team of 220 inspectors—with 50 more to join within weeks—began examining a variety of sites throughout Iraq for the presence of chemical, nuclear, and biological weapons of mass destruction. During the 1990s, Iraq acknowledged having such weapons and weapons development programs. However, Iraqi officials reported that these activities were ended.

The weapons inspection occurring in Iraq in 2003 utilized a variety of weapons detections technologies. Surveillance planes such as the unmanned Predator drone are equipped with high-resolution cameras and provided aerial views of the selected terrain. Detailed images from surveillance satellites placed in orbit over a selected part of the globe provided details of construction projects or the presence of equipment that might be used for weapons. Other cameras were utilized on the ground. Digital cameras can be left in place after an inspection is complete, to provide a longer-term monitoring of the site. Ground penetrating radar positioned on helicopters or unmanned drones was used to seek buried caches of missile components and bunkers that could house weapons. Finally, the portable sensors that have been described were used.

FURTHER READING:

BOOKS:

Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security.* New York: Public Affairs, 2001.

Cirincione, Joseph, Jon B. Wolfsthal, and Jessica T. Mathews. *Deadly Assaults: Tracking Weapons of Mass Destruction.* Washington, D.C.: Carnegie Endowment for International Peace, 2002.

PERIODICALS:

LeDuc, J.W., I. Damar, J.M. Meegan, et al. "Smallpox Research Activities: U.S. Interagency Collaboration 2001." *Emerging and Infectious Diseases* 8 (2002): 743–45.

Reeves, A. "Tracing Biothreats with Molecular Signatures." *Los Alamos National Laboratory Research Quarterly* Fall 2002: 15–17.

ELECTRONIC:

Lawrence Livermore National Laboratory. "Reducing the Threat of Biological Weapons." Chemical/Biological Nonproliferation Program. June 1998. <http://www.llnl.gov/str/Milan.html>(7 January 2003).

SEE ALSO

Anthrax Weaponization
Ballistic Missiles
Biological Warfare
Biosensor Technologies
Chemical Warfare
Pathogens
Spores

Weather Alteration.

SEE *Meteorology and Weather Alteration.*

Windtalkers

ADRIENNE WILMOTH LERNER

Windtalkers was the code name given to the Navajo Indian code talkers employed by United States military intelligence during World War II. Agents developed several encryption methods and code systems during the war, but a code based on the ancient Navajo language was one of

A two-man team of Navajo code talkers attached to a marine regiment in the Pacific relay orders over the field radio using their native Navajo language, a particularly effective code used during World War II. ©CORBIS.

the most successful codes ever used. It remained unbroken throughout the course of the war.

The Navajo code was not the first attempt to use Native American languages to disguise military communications. During World War I, the military adopted the Choctaw language as a code and employed Choctaw code talkers. Indigenous languages attracted code experts because most had no systems of writing and were spoken by a small number of people. The first attempts to utilize Indian languages as code simply involved using the spoken language and translating the messages into English. The language itself functioned as the code, and no additional encryption methods were employed to encipher communications.

In 1939, as World War II began in Europe, the American Army Signal Corps and Naval Intelligence renewed their interest in developing sophisticated enciphering methods. Both Allied and Axis forces relied on new cipher machines and complex mathematical encryption tables for encoding messages. Intelligence service cryptologists broke many of these, such as the German Enigma machine. Codebooks were risky, and too easily recovered by enemy forces. These developments forced cryptologists to change codes often, requiring tedious work. Code experts sought a code that would be simple to use, functional, and secure for the duration of the war.

World War I veteran and civil engineer Philip Johnston proposed the use of a Native American language in conjunction with a letter-symbol replacement encryption system. The son of a missionary, Johnston was raised on a Navajo reservation and spoke the Navajo language fluently. He thought the indigenous language a perfect candidate to use as the basis for a code, largely because of its obscurity. The language had never developed a system of writing, but possessed a great flexibility in its descriptive word combinations. In addition, Navajo men served in cooperation with American forces in World War I, despite tensions during the era between the American government and Indian nations. Military intelligence accepted Johnston's proposal. The project was granted to the Marine Corps for development and supervision. In 1941, the first twenty-nine Navajo code talkers were recruited into service as Marine Corps Radio Operators.

The first twenty-nine recruits worked with Johnston and Marine Corps officials to develop the Navajo language-based code eventually used in the Pacific theater of war. The initial draft of the code consisted of 211 key words and military terms. For the names of places and people, the code used Navajo words to spell out proper nouns by taking the first letter of the word's English equivalent. Because several words could be used to represent one letter in the Latin alphabet, the code was flexible for knowledgeable users, but enigmatic to code breakers. The Navajo code talkers also had to invent Navajo words to represent frequently used military terms. For example, because the Navajo had no word for submarine, they used *besh-lo*, literally meaning "iron fish." Eventually, most radio transmissions were encoded using the word-for-letter replacement system. In 1943, Navajo code talker units experimented with overlaying the Navajo code with a mathematical encryption system. While this method was used with great success to guard classified and highly secret wire transmissions, and could be used in conjunction with cipher machines, the process was too tedious for rapid, battlefield communication.

After months of developing a functional code, the original Navajo code talkers reported for basic training at Camp Elliot, California, in May 1942. Three months later, on August 7, twenty-seven code talkers, designated the 382nd Platoon, departed for their first assignment among the invasion forces at Guadalcanal. The code was used during the battle with great success. Commanding officers complained that other ciphered messages took two hours to send and decode. The Navajo code efficiently transmitted communications in mere minutes. After the battle, the Marine Corps established a radio and wire transmission station for the Pacific fleet. Within weeks, use of the Navajo code increased, eventually encompassing a quarter of all communications sent from the station. The Navajo code also became the cryptological method of choice for urgent communications on the front lines. Realizing the need for more personnel skilled in the Navajo language and trained for code talking, the military founded the Navajo Code Talkers Program at Camp Pendleton,

California. There, Navajo recruits memorized the complex code, and completed specialized equipment training.

Over 540 Navajo served in the Marines during World War II, nearly 300 served in the field as code and communication experts. Navajo code talkers operated in all six Marine divisions, and served in every major Pacific battle between 1942 and 1945. At the battle of Iwo Jima, a small unit of six Navajo code talkers, under the command of 5th Marine Division signal officer, Major Howard Connor, transmitted and received nearly 1,000 messages in 48 hours. The unit garnered a reputation for working ceaselessly, and without error. The security of the Navajo code, in conjunction with the work of American cryptologists who broke several important Japanese codes, gave the Allied forces a decisive intelligence advantage in the Pacific.

Johnston's code was as functional and unbreakable as he originally asserted. The code not only remained uncracked throughout the course of World War II, but also was used in the Korean and Vietnam Wars with similar success. Other indigenous languages, such as those of the Choctaw, Chippewa, Creek, Sioux, and other tribes, were explored as possible sources for military codes both before and after World War II. However, none were more widely used or accomplished than the Navajo code. The code was eventually retired from use and declassified in 1968.

On July 26, 2001, Congress awarded the Congressional Gold Medal to the original twenty-nine Navajo code talkers who aided in the development in the code. The remaining veteran Windtalkers were awarded the Congressional Silver Medal.

FURTHER READING:

BOOKS:

Bixler, Margaret T. *Winds of Freedom: The Story of the Navajo Code Talkers of World War II.* Darien, CT: Two Bytes Publishing Company, 1992.

Kawano, Kenji. *Warriors: Navajo Code Talkers.* Flagstaff, AZ: Northland, 1990.

PERIODICALS:

Watson, Bruce. "Navajo Code Talkers: A Few Good Men." *Smithsonian.* 24, no.5, August 1993.

SEE ALSO

Codes and Ciphers
Codes, Fast and Scalable Scientific Computation
World War II, United States Breaking of Japanese Naval Codes

Wire Tap.

SEE *Bugs (microphones) and Bug Detectors.*

World Health Organization (WHO)

BRIAN D. HOYLE

The World Health Organization (WHO) is the principal international organization managing public health-related issues on a global scale. Headquartered in Geneva, the WHO is comprised of 191 member states (e.g., countries) from around the globe. The organization contributes to international public health in areas including disease prevention and control, promotion of good health, addressing disease outbreaks, initiatives to eliminate diseases (e.g., vaccination programs), and development of treatment and prevention standards.

In 2003, WHO began to coordinate global efforts to monitor the outbreak of the virus responsible for Severe Acute Respiratory Syndrome (SARS). WHO officials also directed aspects of research efforts to identify the specific virus responsible. In addition, WHO officials issued specific recommendations with regard to isolation and quarantine policy and issued alerts for travelers.

Just after the end of World War I, the League of Nations was created to promote peace and security in the aftermath of the war. One of the mandates of the League of Nations was the prevention and control of disease around the world. The Health Organization of the League of Nations was established for this purpose, and was headquartered in Geneva. In 1945, the United Nations Conference on International Organization in San Francisco approved a motion put forth by Brazil and China to establish a new and independent international organization devoted to public health. The proposed organization was meant to unite the number of disparate health organizations that had been established in various countries around the world. The following year this resolution was formally enacted at the International Health Conference in New York, and the Constitution of the World Health organization was approved.

In its constitution, WHO defines health as not merely the absence of disease. A definition that subsequently paved the way for WHO's involvement in the preventative aspects of disease.

From its inception, WHO has been involved in public health campaigns that focused on the improvement of sanitary conditions. In 1951, the Fourth World Health Assembly adopted a WHO document proposing new international sanitary regulations. Additionally, WHO mounted extensive vaccination campaigns against a number of diseases of microbial origin, including poliomyelitis, measles, diphtheria, whooping cough, tetanus, tuberculosis, and smallpox. The latter campaign has been extremely successful, with the last known natural case of smallpox having occurred in 1977. The elimination of

poliomyelitis is expected by the end of the first decade of the twenty-first century.

Another noteworthy initiative of WHO has been the Global Program on AIDS, which was launched in 1987. The participation of WHO and agencies such as the Centers for Disease Control and Prevention is necessary to adequately address AIDS, because the disease is prevalent in under-developed countries where access to medical care and health promotion is limited.

Today, WHO is structured as eight divisions addressing communicable diseases, noncommunicable diseases and mental health, family and community health, sustainable development and health environments, health technology and pharmaceuticals, and policy development. These divisions support the four pillars of WHO: worldwide guidance in health, worldwide development of improved standards of health, cooperation with governments in strengthening national health programs, and, development of improved health technologies, information, and standards.

FURTHER READING:

ELECTRONIC:

World Health Organization. May, 2003.<http://www.who.int/en/> (May 10, 2003).

SEE ALSO

CDC (United States Centers for Disease Control and Prevention)
Public Health Service (PHS), United States

World Trade Center, 1993 Terrorist Attack

JUDSON KNIGHT

The World Trade Center (WTC) bombing of 1993 has long since been overshadowed by the attack that brought the twin towers down on September 11, 2001. Yet, at the time it occurred, the attack loomed as large on the American landscape as the towers themselves once did on the Manhattan skyline. The attack killed six people and injured more than a thousand, the first casualties from foreign terrorists on U.S. soil. American authorities identified at least eight perpetrators, but questions remain as to the ultimate cause of the attack.

The attack and its aftermath. At 12:18 p.m. on Friday, February 26, 1993, an explosion rocked the second level of the parking basement beneath Trade Tower One. The explosive material, as investigators would later determine, was somewhere between 1,200 and 1,500 pounds (544–680 kg) of urea nitrate, a homemade fertilizer-based explosive.

The blast ripped open a crater 150 feet (46 m) in diameter and five floors deep, rupturing sewer and water mains and cutting off electricity. Over the hours that followed, more than 50,000 people were evacuated from the Trade Center complex. A stunned nation soon grasped a fact larger than the incident itself: foreign-sponsored terrorism—which had long plagued Western Europe and parts of the Middle East, Africa, and Asia—had come to the United States.

Investigation and cleanup begins. The first analysis team to arrive came from the Federal Bureau of Investigation (FBI), who soon brought in two examiners from the FBI Laboratory Explosives Unit. Over the week that followed, a team of more than 300 law-enforcement officers from various agencies throughout the country would sift through some 2,500 cubic yards (1,911 cubic meters) of debris weighing more than 6,800 tons (6,909 tonnes).

At the same time that this forensic investigation began, government authorities rushed to protect against physical, chemical, and biological hazards associated with the blast. The explosion had exposed raw sewage, asbestos, mineral wool, acid, and fumes from automobiles. Meanwhile, small electrical fires burned, and pieces of concrete and sharp metal hung threateningly from distended beams.

On Saturday, authorities installed seismographic equipment, cleared the area, and conducted a test run of an empty subway train. The results showed that with a few adjustments, the area could be rendered safe for the operation of the Port Authority Transportation system (PATH) on Monday, thus preventing a virtual shutdown of lower Manhattan. The Environmental Protection Agency and the Occupational Safety and Health Administration began taking steps to clean up biological and chemical debris.

Tracking the killers. Meanwhile, the forensic investigation expanded, with two chemists each from the FBI, ATF (Bureau of Alcohol, Tobacco, and Firearms), and New York Police Department collecting and studying residue from the blast area. In the course of this work, investigators found a key piece of evidence: a 300-pound (136-kg) fragment of a vehicle that, based on the damage it had sustained, must have been at the very epicenter of the blast. Sewage contamination had rendered it unusable for residue analysis, but it bore something much better: a vehicle identification number (VIN).

This was not to be the first fortunate break for investigators. Authorities traced the vehicle to a Ryder truck rental facility in Jersey City, New Jersey, from which it had been reported stolen. On Monday, while FBI special agents were at the Jersey City facility to speak with personnel there, the Ryder clerk received a call from a man identified as Mohamed Salemeh. The latter demanded the return of

FBI agents view the damage caused by the 1993 terrorist bombing of the parking garage at the World Trade Center towers in New York. ©REUTERS NEWMEDIA INC./CORBIS.

his $400 deposit for the van in question, and the Ryder clerk arranged for him to return and collect the deposit on March 4, 1993. When Salemeh arrived, he was arrested.

A search of Salemeh's belongings led investigators to Nidal Ayad, a chemist working for the Allied Signal Corporation in New Jersey. Toll records and receipts helped lead to a safe house in Jersey City, New Jersey, where authorities found traces of nitroglycerine and urea nitrate. They also uncovered evidence that Salemeh and Ayad had obtained three tanks of compressed hydrogen gas, and in the course of searching a storage room rented by Salemeh, investigators found large caches of urea, sulfuric acid, and other chemicals used in making a bomb. On March 3, the *New York Times* received a letter claiming responsibility for the bombing, and subsequent investigation of DNA samples matched Ayad with the saliva on the envelope flap.

Conviction–and continuing questions. The trail of investigation would eventually lead to Ramzi Yousef, who authorities believe was in the van that delivered the explosives to the WTC. With him was Eyad Ismoil. Also implicated in the bombing, along with Salemeh and Ayad, were Ahmad Ajaj, Mahmoud Abouhalima, and Abdul Rahman Yasin. On March 4, 1994, a jury found Salemeh, Ajaj, Abouhalima, and Ayad guilty on 38 counts, including murder and conspiracy, and the judge handed down multiple life sentences.

Yousef fled the country, and engaged in other terror plots before he was captured and brought to the United States from Pakistan in February 1995. He was sentenced to life plus 240 years. As of 2003, Yasin had not been captured, and was believed to be in Iraq. In October 1995, Sheikh Omar Abdel Rahman, a blind Egyptian cleric who taught at mosques in Brooklyn and New Jersey, was sentenced to life imprisonment for masterminding the attack. But some observers wonder whether the roots of the 1993 WTC attack run much deeper.

The fact that Yousef is the nephew of Khalid Sheikh Mohammed, a top figure in al-Qaeda, suggests a strong connection between the 1993 conspirators and the group who ultimately brought down the towers eight years later. After the September 2001, attack, it was the opinion of many investigators and analysts inside President George W. Bush's administration, that the perpetrators of that attack had a state sponsor—Iraq. A number of details,

including the fact that Yousef was traveling on an Iraqi passport, as well as the date of the 1993 attack—the second anniversary of the U.S. liberation of Kuwait in the Persian Gulf War—furthered suspicions of Iraqi involvement in the 1993 incident. Mohammed was later involved in masterminding the terrorist attacks on the World Trade Center in 2001, and was arrested in Rawalpindi, Pakistan on March 1, 2003.

FURTHER READING:

BOOKS:

Dwyer, Jim. *Two Seconds Under the World: Terror Comes to America.* New York: Crown Publishers, 1994.

Gillespie, Angus K. *Twin Towers: The Life of New York City's World Trade Center.* New Brunswick, NJ: Rutgers University Press, 1999.

Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence.* Berkeley: University of California Press, 2000.

Mylroie, Laurie. *Study of Revenge: The First World Trade Center Attack and Saddam Hussein's War against America.* Washington, D.C.: AEI Press, 2001.

Reeve, Simon. *The New Jackals: Ramzi Yousef, Osama bin Laden, and the Future of Terrorism.* Boston: Northeastern University Press, 1999.

ELECTRONIC:

Hirschkorn, Phil. Top Terrorist Convictions Upheld. Cable News Network. <http://www.cnn.com/2003/LAW/04/04/terrorism.yousef/> (April 7, 2003).

SEE ALSO

Bomb Damage, Forensic Assessment
Clinton Administration (1993–2001), United States National Security Policy
United States, Counter-terrorism Policy
Terrorist and Para-State Organizations
World Trade Center, 2001 Terrorist Attack

World Trade Center, 2001 Terrorist Attack

JUDSON KNIGHT

At 8:46 a.m. on September 11, 2001, American Airlines Flight 11, hijacked from Boston's Logan Airport with 92 people on board, crashed into the upper floors of the World Trade Center north tower in lower Manhattan, New York. Seventeen minutes later, United Airlines Flight 175, also hijacked from Logan and with 65 people on board, crashed into the south tower. By this time, virtually the entire nation had tuned in to witness the after-effects on television of what at first seemed a terrible accident, but was quickly revealed as a terrorist attack. Over the course of the next 85 minutes, the south tower collapsed, followed by the collapse of the north tower. The incident, in which nearly 3,000 people died, ranks as by far the worst case of mass murder in U.S. history, the worst building disaster in human history, and the largest terrorist incident in the history of the western world.

The Towers and their Environment

Designed by architect Minoru Yamasaki—who, ironically, had a fear of heights—and engineered by Leslie Robertson and John Skilling, the 110-story towers soared 1,360 feet (415 m) above an open plaza, which made them the world's tallest buildings at the time of their completion in 1973. Whereas the Empire State Building and other older skyscrapers drew support from an interior grid of steel girders, support for the trade towers came from the exterior and the inner core. Horizontal floor trusses joined the perimeter support structure to the central area, which the engineers envisioned as a great "tube" running through the building and containing not only its support structure, but also its utilities such as elevators. This design had two advantages; it made the buildings extremely stable—not prone to swaying in high winds as the Empire State did—and it left much of the interior available as rentable space.

To support such a structure required a strong foundation, and in this regard, the location in lower Manhattan was not a promising one. Bedrock lay between 55 and 80 feet (17–24 m) below street level, and to get to it, construction crews had to deal with another engineering challenge: flooding from the nearby Hudson River. In order to dig without flooding the site, they dug narrow trenches to the bedrock, and as they went, they pumped in a slurry of water and bentonite, a type of clay that expanded to prevent groundwater from flowing in. The slurry trench method made it possible to build a watertight framework for the excavation of the foundation structure, nicknamed "the bathtub."

Excavation began in 1966, and yielded such a quantity of fill that it was used to reclaim 28 acres (11.3 hectares) from the Hudson to form Battery Park City. In addition to supports, in the area underneath the buildings would be seven stories of parking decks, stores, and subway lines. The erection of the buildings themselves, which took more than five years, was a massive feat of both construction and logistics, involving 200,000 tons (181,437) of steel, each major piece of which was marked with an identification number. Over the years of building, many businesses moved in long before the towers were officially completed.

28 years in the towers' lives. On April 4, 1973, the World Trade Center officially opened for business. Though the towers were by far the most notable aspect of the project, they were just two of seven buildings in the entire complex. Built at a cost of $1 billion, the towers functioned as

virtual cities unto themselves, with some 500 businesses, including banks and their offices, law firms, brokerage houses, television stations, charitable organizations, airlines, and government offices. Supporting these functions and the 50,000 employees who filled them were numerous restaurants—most notable of which was "Windows on the World" at the top of the North Tower—as well as other services, including nine chapels of different faiths.

By the 1980s, New Yorkers had become accustomed to the trade towers, which punctuated the skyline as the ultimate symbol of American commerce. Then, in February 1993, just months before the towers turned 20, the towers became the target for a bombing by Islamist terrorists operating a van filled with explosives. In this, the first terrorist attack, six people were killed, but the structural integrity of the towers themselves was not threatened.

September 11 and Its Aftermath

Because of the 1993 attack, many Americans who witnessed the events of September 11, 2001, quickly realized that the buildings had once again become the target for terrorists. When Flight 11 crashed into the North Tower of the World Trade Center at 8:46 a.m., smoke and flames began to gush from the upper stories, and workers began to evacuate the lower floors. Some, however, chose to remain at their desks. For workers on the floors above the impact area, there was no choice but to remain in place.

For 17 minutes, it was possible to assume that what had happened to the North Tower was an accident; then, Flight 175 smashed into the South Tower. Once again, smoke and flames erupted from the heights of the building, and tenants down below began a slow, but steady evacuation while others—many with no choice—stayed where they were.

By 9:59 a.m., millions of Americans had turned on their television sets to watch live reports from the site. Thus, there was a vast audience to experience what happened next, an event that would be etched upon the consciousness of an entire nation. With little warning, the South Tower, succumbing to the stress caused by the fire, began to crash from the top down, creating a vast cloud of dust and ash above and filling the streets below with noise and heat and terror.

By 10:28 a.m., the North Tower began to implode, once again crashing downward from the top, and the area around what had once been the World Trade Center became smoke, ash, and dust. The other five buildings in the former World Trade Center complex, including the Marriott Hotel, the Commodities Exchange, Dean Witter, the U.S. Customs House, and 7 World Trade Center, were destroyed as well. The last of these caught fire, and collapsed that night.

Rescue, cleanup, and the death toll. In the next days and weeks, some 1,500 firemen, search and rescue workers, ironworkers, engineers, heavy equipment operators, and others labored at the site where the towers had stood, a place now known variously as "Ground Zero" or "the Hole." In the shock and horror that followed the attacks, among the few bright spots were the many tales of heroism told by people who owed their lives to police, fire, and medical personnel.

That heroism continued in the weeks of the cleanup, as rescue workers sifted through piles of wreckage. The purpose of their job was manifold. Not only were they cleaning the site, but they were looking for evidence, and—most poignantly—for any signs of the dead.

At first, rescuers had hoped to find survivors trapped under the rubble and trauma centers at local hospitals braced to treat mass casualties, but those hopes faded quickly, and the cleanup work involved sifting through materials that included physical traces of the building's former inhabitants. Not only was the cleanup work grisly, it was also dangerous: rather than working on solid ground, the rescuers had to set up their cranes and other equipment on top of debris piled several hundred feet above the buildings' foundations.

The numbers of the dead would emerge slowly, and had yet to be fully authenticated even two years later. Although the dead numbered 2801, it was estimated that at the early morning hour, almost 7000 of the 50,000 people who worked in the buildings were in their offices at the time of the attacks. Although the span of time between the attacks and the collapse of the buildings was little more than an hour, it had been enough for those who were able to do so to evacuate via stairwells.

Structural explanations. In late 2001, a team of investigators that included representatives of the American Society of Civil Engineers and the Federal Emergency Management Agency (FEMA) commenced a study on the structural collapse of the towers, the details of which they made public in April 2002. In August 2002, the National Institute of Standards and Technology (NIST) began its own study, scheduled to last two years.

The first team concluded that it was not the impact, but the heat from the burning jet fuel, that heated the temperature of the buildings' steel support structures up to 800°C (1472°F), causing them to buckle and the floors to collapse downward. (Both jets were bound for Los Angeles and had almost a full complement of fuel on board.) On the other hand, the impact did have the effect of knocking out support columns in the building's interior, which may have weakened the structure. The initial crash neutralized sprinkler systems, allowing spread of the fire, which was fed by caches of paper and other flammable materials in offices.

Almost all sources, including government officials, architects, and engineers, agreed on key elements of the building damage. First, it would have been virtually impossible to prevent the destruction of the buildings by

aircraft used in the way they were on September 11 as guided missiles. Second, the structural integrity of the buildings that allowed the towers to stand for over an hour after the impacts enabled thousands of people to evacuate. Finally, it was evident that the era of the extremely tall skyscraper was in question. Due to high costs, the construction of very tall buildings had been on the decline in the United States for many years, and the events of 9/11 sealed the fate of some mega-skyscraper projects.

The perpetrators. Federal authorities, using financial records and other materials, had long since identified the al-Qaeda terror network as the perpetrators of the attack. Al-Qaeda was not a new name: it and its leader, Osama bin Laden, had been linked with the August 1998 bombings at U.S. embassies in Africa, and with the bombing of the USS *Cole* in Yemen in 2000.

Al-Qaeda had strong links to the Taliban regime in Afghanistan, which gave them asylum. Officials in the administration of President George W. Bush, as well as some observers outside the administration, also held that there were substantive links between al-Qaeda, the terrorists who carried out the 1993 bombing, and the government of Iraq. (In fact, Ramzi Youssef, one of the ring leaders in 1993, was nephew to Khalid Sheikh Mohammed, a top al-Qaeda operative, and considerable evidence—including Youssef's Iraqi passport—linked them to Iraq.) The U.S. military actions against Afghanistan in 2001–2002, and Iraq in 2003, were a response to the 2001 terrorist attacks, whose most potent images revolved around the collapse of the World Trade Center towers.

■ FURTHER READING:

BOOKS:

Halberstam, David. *New York September 11.* New York: PowerHouse Books, 2001.

Hoge, James F., and Gideon Rose. *How Did This Happen?: Terrorism and the New War.* New York: PublicAffairs, 2001.

One Nation: America Remembers September 11, 2001. Boston: Little, Brown, 2001.

Smith, Dennis. *Report from Ground Zero: The Story of the Rescue Efforts at the World Trade Center.* New York: Viking, 2002.

ELECTRONIC:

Day One—The Attack. Los Angeles Times. <http://www.latimes.com/news/nationworld/nation/la-dayone-graphics.story> (April 22, 2003).

September 11, 2001. How Stuff Works. <http://www.howstuffworks.com/sept-eleven3.htm> (April 22, 2003).

September 11 Archive. <http://september11.archive.org/> (April 22, 2003).

SEE ALSO

Enduring Freedom, Operation
FEMA (United States Federal Emergency Management Agency)
Iraqi Freedom, Operation (2003 War against Iraq)
Kenya, Bombing of United States Embassy
NIST (United States National Institute of Standards and Technology)
Patriot Act, United States
Persian Gulf War
September 11 Terrorist Attacks on the United States
Terrorist and Para-State Organizations
United States, Counter-terrorism Policy
USS Cole,
World Trade Center, 1993 Terrorist Attack

World War I

■ ADRIENNE WILMOTH LERNER

World War I, which spanned a four-year period between 1914 and 1918, erupted as a result of the complicated European alliance system. The assassination of Austrian Archduke Ferdinand, and his wife, Sophie, by Serbian nationalists sparked pan-European conflict when Russia, backed by France, declared their intent to defend Serbia, should Austria declare war. The Austrian government, with its ally Germany, declared war on Serbia three days later. British forces joined the French and Russians, but the United States, home to large immigrant populations of all of the fighting nations, resolved to remain out of the conflict.

The United States declared its neutrality, but the nation harbored Allied sympathies. United States manufacture and trafficking of munitions and supplies to aid British and French forces angered Germany and Austria. The German Navy attacked American ships, potentially loaded with contraband, in the Atlantic, and sent intelligence agents to conduct sabotage operations within the United States. In 1917, German hostility prompted the United States to enter the conflict in Europe.

The war ended in 1918, followed by the formal surrender of German and Austrian forces with the signing of the Treaty of Versailles. However, World War I forever changed modern warfare, introducing the concepts of total warfare and weapons of mass destruction.

National intelligence communities. At the outbreak of the war, many nations had weak or fledgling national intelligence communities. The French government and military both maintained trained intelligence forces, but no central agency processed intelligence information, or facilitated the distribution of critical intelligence information. Russia had special agents of the Czar, and secret police forces, but its foreign intelligence infrastructure was almost nonexistent.

Members of the first contingent of New Yorkers drafted into the United States Army are shown lined up in front of their barracks at Camp Upton, Long Island, New York, as America enters World War I in 1917. AP/WIDE WORLD PHOTOS.

The United States developed stronger domestic intelligence and investigative services in the decade before World War I. However, the country's lingering isolationism and neutral posture in the war hampered the development of a foreign intelligence corps until the United States entered the war in 1917.

Britain had a well-developed military intelligence system, coordinated through the Office of Military Intelligence. British intelligence forces engaged in a range of specialized intelligence activities, from wiretapping to human espionage. The vast expanse of British colonial holdings across the globe provided numerous outposts for intelligence operations, and facilitated espionage. British forces were among the first to employ a unit of agents devoted to the practice of industrial espionage, conducting wartime surveillance of German weapons manufacturing.

Of all the warring nations in 1914, Germany possessed the most developed, sophisticated, and extensive intelligence community. The civilian German intelligence service, the *Abwehr*, employed a comprehensive network of spies and informants across Europe, North Africa, the Middle East, and in the United States. German intelligence successfully employed wire taps, infiltrating many foreign government offices before the outbreak of the war.

World War I forced most national intelligence services to rapidly modernize, revising espionage and intelligence tradecraft to fit changing battlefield tactics and technological advances. The experience of the war formed the first modern intelligence services, serving as forbearers of the intelligence communities in France, Britain, Germany, and the Untied States today.

Sabotage. German intelligence trained special agents, most of whom used professional or diplomatic covers in the United States, to conduct acts of sabotage against United States industries that aided the British, French, and Russian allied forces in the war. International rules of engagement limited the ways in which Germany and Austria-Hungary could provoke or attack the declaredly neutral United States. German high command desired to cripple United States aid capabilities, but not provoke the nation to enter the conflict. German undercover agents attacked railroads, warehouses, shipyards, and military instillations in 1914 and 1915. Agents attempted to make these attacks appear as accidents, but United States authorities caught several potential saboteurs before they destroyed property, unmasking the German plot. Anti-spy hysteria fueled

public fear and anger regarding the acts of German saboteurs.

German and Austrian agents carried out more than 50 acts of sabotage against United States targets on American soil during the course of the war. Most of the attacks occurred in New York City and the region surrounding New York harbor. The most famous and devastating attack, the sabotage of Black Tom Pier, shook buildings and broke windows across New York City and suburban New Jersey. The July 29, 1916, explosion destroyed several ships and waterfront ammunition storage facilities. The attack decimated Black Tom Pier, the staging area for most shipments bound for the Western Front in Europe.

German sabotage attacks in the United States, while successful, only managed to strike at a handful of military and shipping targets. The United States government continued to aid British and French forces in Europe, but the attacks inflamed pro-war sentiment.

Communications and cryptology. Advancements in communications and transportation necessitated the development of new means of protecting messages from falling into enemy hands. Though an ancient art, cryptology evolved to fit modern communication needs during World War I. The telegraph aided long-distance communication between command and the battlefront, but lines were vulnerable to enemy tapping. All parties in the conflict relied heavily on codes to protect sensitive information. Cryptology, the science of codes, advanced considerably during the first year of the war. Complex mathematical codes took the place of any older, simple replacement and substitution codes. Breaking the new codes required the employment of cryptology experts trained in mathematics, logic, or modern languages. As the operation of codes became more involved, the necessity for centralized cryptanalysis bureaus became evident. These bureaus employed code breakers, translators, counterintelligence personnel, and agents of espionage.

The most common codes used during the war continued to be substitution codes. However, most important messages were encrypted. Encryption further disguised messages by applying a second, mathematical code to the encoded message. Encryption and coding both required the use of codebooks to send and receive messages. These books proved to be a security liability for the military. During the course of the war, four separate German diplomatic and military corps code books fell into the hands of British intelligence, compromising the security of German communications for the rest of the war.

Both the Germans and the British broke each other's World War I codes with varying success. The German *Abwehr* broke several British diplomatic and Naval codes, permitting German U-boats to track and sink ships containing munitions. British cryptanalysis forces at Room 40, the military intelligence code-breaking bureau, successfully deciphered numerous German codes, thanks in large part to the capture of German codebooks. In 1917, British intelligence intercepted a diplomatic message between Berlin and Mexico City, relayed through Washington. The message, known as the Zimmerman Telegram, noted German plans to conduct unrestricted warfare against American ships in the Atlantic, and offered to return parts of Texas and California to Mexico in exchange for their assistance. Discovery of the Zimmerman Telegram prompted the United States to enter World War I.

Cryptology, once the exclusive tool of diplomats and military leaders, became the responsibility of the modern intelligence community. After World War I, many nations dissolved their wartime intelligence services, but kept their cryptanalysis bureaus, a nod to the growing importance of communications intelligence and espionage.

Trench warfare and the evolution of strategic espionage tradecraft. The advent of trench warfare necessitated the development of new surveillance and espionage techniques to locate enemy positions and gauge troop strength. Crossing "no man's land," the area between trench fronts, was dangerous, and using human scouts proved costly to both sides in the early months of the war. Military intelligence officers instead relied on networks of local citizens for information on enemy advances and supply lines. Finding sympathetic locals was possible for both sides in the trenches of Northern France, as the battlefront crossed the linguistically and culturally diverse German-French region of Alsace-Lorraine.

The airplane was a new invention when war broke out in Europe. Though the device was unproven in war, German commanders recognized that air combat and aerial bombardment were the most significant war tactics of the future. Britain developed fighter squadrons of its own to combat the German air menace. Despite the fame of the German Red Baron and World War I aerial dogfights, airpower was a very small part of the war effort on both sides. However, low-flying airplanes proved invaluable surveillance and intelligence tools, permitting military command to obtain accurate and up-to-date information on enemy trench locations and fortifications. British forces experimented with aerial surveillance photography, trying several cameras, but the medium had little success during the course of World War I.

German and Austrian forces introduced the use of balloons to monitor weather patterns and deliver explosive charges. Sometimes, dummy balloons were sent across enemy lines so that scouts could monitor where individual balloons were shot down, thus mapping probable enemy strongholds. British and French forces soon reciprocated by using balloons of their own, but by the time they introduced the devices, balloons signaled the impending use of a far more sinister weapon, poison gas.

Chemical weapons. Although military strategists during the nineteenth century noted the potential use of poison gas on the battlefield, the development of the first, World War I–era chemical weapon happened by accident. Seeking to

conserve TNT, British and German forces substituted two different agents, Lyddite and Dianisdine salts respectively, into their explosive charges. The chemicals produced a tearing agent and mild respiratory irritant, sending victims into violent fits of sneezing.

The French first developed strong tear gas agents for battlefield use in June 1914. French forces first employed the gas in the form of tear-gas grenades, in August 1914. German scientists created a similar agent, and were the first to research various types of poison gas for extensive battle use. In October 1914, the Germans fired the first gas-filled shells. A few months later, experiments with filled shells were unsuccessful. Gasses failed to properly vaporize on the Eastern Front during the freezing winter. Variable winds on the Western Front made dispersal of gasses difficult.

By 1915, the German, French, and British armies all sought to develop chemical agents that would help end the relentless stalemate of trench warfare. Outdated battlefield tactics ordered soldiers to charge fortified trenches, across open fields strewn with barbed wire. Military commanders hoped poison gas would help soften or destroy manned defenses, permitting successful seizure of enemy positions.

The first major use of strong poison gas was an asphyxiant and respiratory irritant, chlorine, at the Second Battle of Ypres. German forces mounted a heavy bombardment of the French, British, and Algerian Ypres Salient. In the evening, the firing grew more intense, and Algerian troops noticed a peculiar yellow cloud drifting toward the Salient. French military commanders believed the yellow smoke hid an oncoming German advance, so soldiers were ordered to stand their ground and man machine gun defenses. As a result, many men died and the Salient was broken, forcing the Allies to retreat.

Germany drew immediate criticism for its inhumane use of gas on the battlefield. German diplomats assured rival powers that poison gas would be used regularly against their forces, provoking further condemnation. Both sides of the conflict employed agents of espionage to spy on the production of new weapons. Informants told Allied authorities about the possible German use of chlorine gas at Ypres. After Ypres, intelligence personnel changed its tactics to obtain specific information on the gasses each side was producing, and how they intended to weaponize the chemicals.

The British government commissioned Special Gas Companies to create poisons for wartime uses. On September 24, 1915, Allied forces retaliated the initial German gas attacks. Setting some 400 chlorine gas canisters along the German lines at Loos, British forces began the gas attack at dawn. A few minutes after sunrise, the prevailing winds suddenly shifted, driving the cloud of gas back over British lines. The operation was disastrous, Britain suffered more causalities on the day than did Germany.

After the incident at Loos and several similar gas reversals, both British and German forces experimented with different means of delivering poison gasses to minimize friendly-fire exposure to the chemicals. The creation of stronger, more deadly agents, such as Phosgene (an asphyxiant) and later Mustard Gas (a blister agent that burned exposed skin and eyes), necessitated a remote delivery system. Gas canisters were dropped from balloons and airplanes, but the system was not always reliable and targeting specific locations was difficult. Advancement in ammunition design, and the chemical agents themselves, finally permitted chemical agents to be placed in the payload of long-range artillery shells.

Despite more efficient delivery mechanisms, chemical warfare eventually became less effective on the battlefield. All armies in the conflict quickly devised protective gear to shield soldiers from exposure to chemical agents. Cotton wraps dipped in baking soda and gas masks greatly reduced the number of casualties from most gasses, though they offered no protection from the increasingly used Mustard Gas. Battlefield toxins became more deadly, especially with the limited use of cyanide derivatives and prussic acid, a crippling nerve gas. However, protective clothing and gas masks limited mortality from rare gasses.

Better intelligence also helped combat casualties incurred from gas attacks. Intelligence aided troops in the trenches to reposition to avoid an impending attack. Identification of the type of gasses possessed by the immediate enemy corps further detracted from the element of surprise, upon which gas attacks heavily relied. Despite its diminished success, gas continued to be regularly deployed.

The legacy of World War I. By the end of World War I, over 100,000 people were killed, and one million injured, by poison gas attacks. Those injured often suffered debilitating injuries, creating further public ire for chemical weapons. Civilians were inadvertently injured by contaminated areas, especially by the long-lingering mustard gas. After the war, the newly established League of Nations moved to amend the international rules of engagement to disallow the use of poison gas. Though the motion gained public and diplomatic support, military leaders were hesitant to agree to a total ban on chemical warfare. In 1925, the Geneva Protocol outlawed the use of chemical and biological weapons in war against human targets. However, the treaty did not prevent their further use, and chemical and biological weapons attacks by rogue nations or terrorist organizations have now reemerged as a global threat.

The Armistice created the political map of Europe that sparked the powder keg of World War II. The German government collapsed under the weight of reparation payments and hyperinflation, only to emerge from economic troubles under the reign of Adolf Hitler and his Nazi Party. In the East, small ethnic nations were combined into larger states, embittering nationalists that hoped the war would bring freedom from Austrian, Russian, or German domination. Russia began a tumultuous revolution in

1917, withdrawing from the war to concentrate on domestic affairs.

The legacy of World War I extends beyond World War II, however. Many nations participating in the conflict realized the necessity for some sort of permanent intelligence services, whether cryptology and surveillance units, or large government intelligence agencies. The nature of war, and the business of intelligence in wartime and peacetime were altered by the events of World War I.

FURTHER READING:

BOOKS:

Gilbert, Martin. *The First World War: A Complete History.* New York: Henry Holt, 1996.

Keegan, John. *The First World War.* New York: Vintage Books, 2000.

SEE ALSO

Black Tom Explosion
Room 40
World War I: Loss of the German Codebook

World War I: Loss of the German Codebook

ADRIENNE WILMOTH LERNER

At the outset of World War I, the science of cryptography assumed a distinctly modern character. New developments, such as the international telegraph system and the telephone left cryptologists grappling with new ways to adapt encryption methods to the new technology. The ultimate goal of cryptologists of the era was to invent a means of transcribing and decoding ciphers without the use of cumbersome codebooks that could easily fall into enemy hands. Wartime experimentation proved impractical, so for most of the war, both sides relied on older-style codebooks. For the Germans, this proved disastrous. Between 1914 and 1918, the German forces lost four codebooks, all of which were recovered by British intelligence services. For much of the war, German communications were intercepted and deciphered by the British intelligence code-breaking unit known as Room Forty, giving Allied forces a decisive strategic advantage.

The first copy of a German codebook to be recovered by British forces was stolen with the help of British-born Austrian spy, Alexander Szek. Szek was a telegraph operator in Belgium. Room Forty picked up strange signals coming from Szek's station, then contacted Szek, along with locating his relatives in London. British agents sent a letter to Szek, urging him to join the British war effort as a spy, or face unforeseen consequences. They further threatened to incarcerate his relatives who lived in London.

Szek agreed to help steal German codes by photographing the German codebook. He was intensely nervous about his espionage role for the beginning of the operation, but became even more unnerved as time progressed. Fearing capture by the Germans, Szek arranged with intelligence officers to flee to Britain after he completed his work photographing the codebook. When Szek delivered the last copies of the codebook to an agent in the Netherlands, however, he was returned to Brussels so as not to appear suspicious to German authorities. If the Germans suspected that Szek had stolen the code, the code would be replaced. His jumpy actions rendered Szek a security risk.

Szek was later found shot to death in his apartment in Brussels. The British government claimed that German agents killed Szek after discovering his espionage activities. Unaware of the theft, the Germans continued to use the code Szek had stolen. Some years later, British Navy captain and intelligence attaché Captain Stephen Roskill, admitted to ordering a hired hit on Szek. The British Admiralty was plagued by Szek's constant nervousness and worried that he might confess his actions to the Germans in order to assuage his sense of guilt. Although the information gained from Szek's work was immensely valuable, its price would soon seem exceedingly steep. A few months after incident with Szek, British divers recovered a box from a sunken German U-boat. The box contained a copy of the German Foreign Office code book, the same code that had been laboriously photographed and smuggled to British intelligence by Szek.

1914 was a providential year for Room Forty. In August, a third German codebook, the naval code, was given to British cryptologists by Russian forces. The German cruiser Magdeburg sank off the coast of Finland, and a Russian vessel picked up survivors of the downed ship. Upon searching the German crew, Russian authorities discovered the codebook in the possession of one of the ship's officers. After analyzing the new codebooks, British intelligence was able to decipher and monitor most German fleet dispatches from 1915 to 1917, after which a variant code was introduced.

Room Forty cryptologists received one final gift in 1915. As British forces closed in on Persia, German consul Wilhelm Wassmus hastily fled his office, leaving behind his copy of the German diplomatic codebook. While the code was less frequently used than others, the recovery of the fourth code book gave Room Forty the mathematical key to the main German encryption system.

With a network of listening stations established in Europe and in the North Sea, Room Forty monitored most German wire traffic throughout the course of the war. The loss of codebooks diminished Germany's capability for surprise attacks at sea, despite the advantage of a technically superior fleet. In 1918, the German company Siemans,

under contract with the German government, developed a prototype cipher machine that encoded and decoded messages without need of a codebook.

FURTHER READING:

BOOKS:

Gilbert, Martin. *The First World War: A Complete History.* New York: Henry Holt, 1996.

Khan, David. *The Codebreakers: The Story of Secret Writing.* New York: Scribner, 1996.

SEE ALSO

Room 40

World War II

JUDSON KNIGHT

The Second World War was history's largest and most significant armed conflict. It served as the breeding ground for the modern structure of security and intelligence, and for the postwar balance of power that formed the framework for the Cold War. Weapons, materiel, and actual combat, though vital to the Allies' victory over the Axis, did not alone win the war. To a great extent, victory was forged in the work of British and American intelligence services, who ultimately overcame their foes' efforts. Underlying the war of guns and planes was a war of ideas, images, words, and impressions—intangible artifacts of civilization that yielded enormous tangible impact for the peoples of Europe, east Asia, and other regions of the world.

Scope and Consequences of the War

The war pitted some 50 Allied nations, most notable among which were the United States, United Kingdom, Soviet Union, and China, against the Axis nations. The name "Axis," a reference to the straight geographic line between the capital cities of Rome and Berlin, came from a pact signed by Germany and Italy in 1936, to which Japan became a signatory in 1940. Ultimately a number of other nations would, either willingly or unwillingly, throw in their lot with the Axis, but Germany and Japan remained the principal powers in this alliance.

Although the roots of the conflict lay before the 1930s, hostilities officially began with the German invasion of Poland on September 1, 1939, and ended with the Japanese surrender to the United States six years and one day later. The war can be divided into three phases: 1939–41, when Axis victory seemed imminent; 1941–43, when Axis conquests reached their high point even as the tide turned with the U.S. and Soviet entry into the war; and 1943–45, as the Allies beat back and ultimately defeated the Axis.

Over those six years, armies, navies, air units, guerrilla forces, and clandestine units would fight across millions of square miles of sea and land, from Norway's North Cape to the Solomon Islands, and from Iran to Alaska. The war would include more than a dozen significant theatres in western Europe, the north Atlantic, Italy, eastern and southern Europe, Russia, North Africa, China, southern Asia, Southeast Asia, and the Pacific islands. Less major, but still significant, engagements took place in East Africa, the Middle East, and West Africa. There were even extremely limited engagements—mostly at the level of diplomacy, espionage, or propaganda—in South America and southern Africa.

Death toll. World War II and its attendant atrocities would exact an unparalleled human toll, estimated at 50 million military and civilian lives lost. Combat deaths alone add up to about 19 million, with the largest share of this accounted for by 10 million Soviet, 3.5 million German, 2 million Chinese, and 1.5 million Japanese deaths. (The United States lost about 400,000, and the United Kingdom some 280,000.)

Adolf Hitler and the Nazis killed another 15.5 million in a massive campaign of genocide that included the "Final Solution," whereby some 6 million Jews were killed. Another 3 million Soviet prisoners of war, along with smaller numbers of Gypsies, homosexuals, handicapped persons, political prisoners, and other civilians rounded out the total. Principal among the Nazi executioners was the SS, led by Heinrich Himmler, which operated a network of slave-labor and extermination camps throughout central and eastern Europe.

About 14 million civilian deaths have been attributed to the Japanese. They imposed a system of forced labor on the peoples of the region they dubbed the "Greater East Asia Co-Prosperity Sphere," and literally worked millions of civilians and prisoners of war (POWs) to death in their camps. The Japanese also conducted massacres of civilians that rivaled those undertaken by the Nazis in Russia.

Soviet non-combat atrocities accounted for another 7 million deaths. Victims included members of deported nationalities, sent eastward to prevent collaboration with the Nazis; murdered German POWs; returning Soviet POWs killed because of their exposure to the West; and other campaigns of genocide conducted by Soviet dictator Josef Stalin.

World War II served as a watershed between the multi-polar world of the nineteenth and early twentieth centuries, and the bipolar world of the Cold War. It ended the military dominance of European powers, but also

An American medical officer examines the bullet-riddled bodies of three German spies who died before a U.S. firing squad in Herbesthal, Belgium, in December 1944. ©BETTMANN/CORBIS.

ushered in an era in which Europe, heavily aided in its recovery by the United States so as to avoid another European war, became a major economic power.

The war transformed the United States from an isolationist giant, with little interest in affairs outside the Western Hemisphere, to a modern superpower. Symbolic of this transformation was the construction of the Pentagon building, commenced just before the United States entered the war. The war also marked the birth of the modern U.S. intelligence apparatus, of which the Office of Strategic Services (OSS), led by Major General William Donovan, was the progenitor. OSS would cease to function soon after the war's conclusion, but two years later, it would be replaced by a far more lasting organization, the Central Intelligence Agency (CIA).

Despite the wartime alliance with the Soviet Union, and the creation of the United Nations in an effort to settle international differences peacefully, the Cold War was an all but inevitable result of the war, which left only two superpowers in its wake. Thenceforth, the world would be divided between the United States and its allies—among which would be its two wartime enemies, West Germany and Japan—and the Soviet Union and its affiliates. These would include East Germany and eastern Europe; Communist China from 1949 to the Sino-Soviet rift of the late 1950s; and a number of states in the gradually emerging developing world of the Middle East, Africa, and Asia.

The conflict spelled an end to the European colonial empires, and brought independence to dozens of countries in the Middle East, Africa, and south and east Asia. Among the many states that owed their existence to the war was Israel. The effects of the Holocaust moved Western leaders to action, and Western sympathy helped ensure support for the establishment of a Jewish state.

The Axis and the Causes of the War

The victory of Benito Mussolini's Black Shirts in Italy in October 1922, introduced the world to Fascism, which reinterpreted nationalism in totalitarian terms, i.e., as an all-encompassing political movement intended to supplant all other centers of influence, such as religion, in the life of the individual. Hitler regarded Mussolini as a mentor, yet the Nazis would eclipse the Fascists in terms of strength, influence, and impact on world history.

Not only was Germany's militarily more powerful than Italy's, but the agenda of the Nazis, who took power in January 1933, had a much greater sense of urgency.

Poster designed by artist Cliff Parks for Air Cadets at Ellington Field, Texas, the world's largest multi-motor flying school, in 1942. ©BETTMANN/CORBIS.

Central to Hitler's plans, outlined in his manifesto *Mein Kampf* (1924), was the elimination of central and eastern European Jews, who Hitler regarded as the principal barrier to German European dominance. Intimately tied with this plan was his vision of conquest and colonization in Russia and eastern Europe, which would—after the Jews and Slavs had been exterminated—constitute a German empire or *reich* that Hitler predicted would last a thousand years.

This consciously millenarian vision drew on German history and national mythology, citing as the first and second reichs the Holy Roman Empire of the Middle Ages and the German Empire of 1870–1918 respectively. It appealed not only to longstanding strains of anti-Semitism in Europe, which dated back at least to the time of Crusades, but also to disaffection with what the Germans regarded as their betrayal and humiliation in World War I and with the Versailles Treaty of 1919. In a country that had recently been devastated by inflation—Germany's economic crisis preceded the worldwide Great Depression by several years, and was even more severe—Nazism seemed to offer a solution for strengthening a once-great nation that had fallen on difficult times.

Communism and the Spanish Civil War. At a rhetorical and symbolic level, Hitler opposed Communism, and used the threat of Soviet Russia as justification for his moves to arm Germany in the 1930s. In reality, the Nazis and Soviets provided one another with mutual assistance, continuing a pattern begun in World War I, when imperial Germany had aided V. I. Lenin. After the war, German aristocrats, nationalists, and Communists all opposed, and helped bring down, the liberal democratic Weimar Republic. Though Hitler killed thousands of Communists after he gained power in January 1933, German military forces trained in Russia, and Germany provided Russia with equipment.

This secret relationship would become public when the two sides signed the Non-Aggression Pact on August 23, 1939, but until that time, Hitler and Stalin made much of their putative opposition to one another. The Spanish Civil War (1936–39) provided them with a proxy battleground, as Germany and Italy tried out new armaments in support of the Nationalists, led by Francisco Franco. The Republican side turned to Stalin for help, but he gave them little assistance while siphoning resources and leaders, some of whom went to Moscow and never returned.

On the other hand, the romance and mythology of the Republican cause provided the Soviets with a propaganda victory that comported well with their current "Popular Front" strategy. In accordance with the latter, Communists worldwide ceased calls for world revolution, and instead formed alliances with liberal, socialist, and anarchist movements. Later, Stalin would form a "popular front" on a grand scale, as he aligned himself with the United States and Great Britain.

Munich and Mussolini. Hitler's rhetorical opposition to Communism won him tacit support from Britain and France, which in the 1930s regarded Nazism as the lesser of two evils. At Munich in September 1938, British and French complicity yielded Germany title to a portion of Czechoslovakia known as the Sudetenland. In the view of many historians, the Munich conference and the appeasement efforts of British Prime Minister Neville Chamberlain rendered war all but inevitable.

Munich also sealed the relationship between Mussolini and Hitler. Despite their later alliance, Mussolini, a former Communist, rightly perceived significant differences between his nationalism and Hitler's racism. If Britain and France perceived Hitler as a buffer against Stalin, then Mussolini in the early 1930s seemed like a buffer against Hitler. What brought Italy and Germany together was the same complex of factors that eventually forged a three-way alliance with Japan: a shared desire for greater power, territorial ambitions that had supposedly been frustrated by the democratic powers, and a string of diplomatic and military successes that encouraged ever bolder moves.

Japan, militarism, and expansionism. When its troops marched into Manchuria in 1931, Japan launched the first in the series of conquests and invasions during the 1930s that set the stage for the war. Though nominally led by an emperor, Hirohito, by that time the nation had come under the control of military officers, who had imposed a dictatorship. The Japanese lacked a single powerful leader until Hideki Tojo emerged at the top in 1941.

Although certainly authoritarian and strictly controlled, the Japanese system was technically not totalitarian, in the sense that it did not have a specific, animating modern ideology. Instead, it relied on ancient national myths, combined with an abiding sense that Japan had been wronged in its struggle to make a place for itself as a world power. The Japanese belief system combined nationalistic and racial themes: like the Nazis, they regarded all other peoples as inferior. This would have seemingly made the Japanese and Nazi systems mutually exclusive, but because they were at opposite sides of the world, it provided a convenient formula for dividing the planet between them.

Each of the three future participants in the Axis Pact set out to test the resolve of the other powers to oppose them, and found such opposition all but nonexistent. The League of Nations, formed to put an end to wars after World War I, failed to act decisively when Italy conquered Ethiopia in 1935–36, when Germany occupied the Rhineland in 1936, when Japan conquered most of eastern China in 1937–38, or when Germany annexed Austria in 1938.

1939–41: The Axis triumphant. Over the course of the first nine months of 1939, Germany added the rest of Czechoslovakia, while Italy occupied Albania. Having signed the Non-Aggression Pact with Stalin in August, Hitler invaded Poland on September 1. Britain and France, which on

March 29 had pledged to support Poland, declared war, but did not attack Germany. During the next few weeks, Germany and Russia divided Poland between themselves, and in November, the Soviet Union launched a separate war with Finland.

Although the Soviets eventually emerged victorious in March 1940, the Russo-Finnish War convinced Hitler of Stalin's vulnerability. Stalin had decimated his officer corps with his purges in the 1930s, and his collectivization efforts had been accompanied by the imprisonment, starvation, and deaths of millions. The Soviet Union was to prove much stronger, however, than Hitler imagined. And if Hitler believed that Japan would join him in making war on the Soviets, he was mistaken; the Soviet performance against the Japanese during the little-known tank battle at Nomonhan in Manchuria in August, 1939, effectively convinced the Japanese of Russia's true strength.

From 1939 to 1941, the Axis unquestionably had the upper hand in the conflict. During the first part of this period, nicknamed "the Phony War," hardly a shot was fired in western Europe. Only in the spring of 1940 did Hitler's forces resume action, conquering Denmark, Norway, the Low Countries, and France. The French, who relied on the defenses of the Maginot Line (designed to fight a World War I–style conflict of limited movement), surrendered after a nominal resistance effort. Most of the country fell under direct Nazi control, which a small portion to the southeast, with the town of Vichy as its capital, formed a pro-Axis government.

The speedy capitulation of the French left the British alone in opposition to the Nazis. In May 1940, Chamberlain resigned, and was replaced by Winston Churchill. In this change, the British people gained an unexpected advantage; over the next five years, Churchill, widely regarded as one of history's great orators, would stir his people to action with a series of memorable speeches. Yet, the position of the British was perilous, and as the Nazi Luftwaffe launched an aerial campaign against them in August, it seemed that German victory was only a matter of time.

Axis victories and blunders. At about the same time that the Battle of Britain began, Mussolini attacked the British in North and East Africa. He thus unexpectedly offered England a venue for fighting the Axis outside of Europe, and eventually German forces would be diverted into the Africa campaign.

In southern Europe, Hitler managed to compel Bulgaria, Hungary, and Romania into joining the Axis, but this advantage was overshadowed by another diversion of forces caused by Mussolini. Mussolini invaded Greece in October 1940, and Greek resistance proved so fierce that in April 1941, German forces rolled into southern Europe. Churchill attempted to oppose them in Greece, but the Germans pushed back British forces, and in history's first airborne invasion, took the isle of Crete—an important Mediterranean base—in May.

By mid-1941, virtually all of Western Europe, except Britain and neutral Switzerland, Spain, and Sweden, belonged to the Axis. But the Balkan campaign had pushed back Hitler's timetable for the most important campaign of the war, the invasion of Russia. The purpose of all other fighting up to that point had been to eliminate opposition as Germany invaded the Soviet Union, and rather than conquer Britain, Hitler preferred to enlist it as an ally against Stalin. He called off attacks on British air bases in May 1941, but by then the Nazi bombardment had inflamed British sentiment against Germany.

1941–43: The Tide Turns

On June 22, 1941, the Nazis invaded Russia. Operation Barbarossa, as it was called—its name a reference to the twelfth century Holy Roman Emperor Frederick I Barbarossa—was the largest land invasion in history. Fought according to the blitzkrieg ("lightning war") tactics already demonstrated elsewhere in Europe, the invasion relied on mechanized infantry divisions and Panzer (tank) columns with heavy aerial support.

The invasion would initially yield enormous victories for the Nazis, who quickly doubled the size of their territory by annexing most of western Russia. However, the Germans had started the invasion relatively late in the year and were eventually delayed in their advances, given the challenges posed by the Russian winter. This delay was partly due to the incursion into southern Europe, but also resulted from arguments between Hitler and his general staff, which put off the invasion for several weeks.

Not content to be Germany's *Führer* or supreme leader, Hitler also wished to be generalissimo, and eventually he would push aside all military planners and take personal control of the war effort. Not only did Hitler, a corporal in World War I, lack the generals' understanding of strategy, but he tended to be bold where prudence counseled caution, and vice versa. When he had a good chance of taking Britain, he demurred, but a year later, he swept into Russia without taking adequate stock of the consequences.

German troops were not equipped with clothing for the winter. This was in part a consequence of the fact that Hitler resisted apprising his armies or his people of the sacrifices necessary for war. Whereas the Allies immediately undertook rationing efforts, Hitler was slow to enact rationing for fear of unleashing discontent. Likewise, he was ill-inclined to equip his men for a long campaign, and thus admit that such a campaign likely awaited them.

America enters the war. Japan launched its first major offensive of the war in early December 1941, when, in addition to attacking the United States at Pearl Harbor, it swept into the Philippines, Malaya, Thailand, and Burma. The result of these decisive attacks, combined with German victories in Russia, was to bring the Axis to the height of its powers in 1942. At that point, it seemed possible that

the two major Axis powers, taking advantage of anti-British unrest in Iran and India, might even link up, thus controlling a swath of land and sea from Normandy to the Solomon Islands.

In actuality, events of 1941 would serve to bring an end to Axis hopes of world conquest. While the invasion of Russia would ultimately cripple the German Wehrmacht, or army, the introduction of the United States to the war would give the Allied force a seemingly bottomless supply of equipment with which to wage the war. It also brought in a vast military force that, alongside the British, would drive back the Germans in North Africa (despite impressive resistance by the tank commander German Erwin Rommel) and make two key landings on the European continent, in Italy and France.

Thus, the attack on Pearl Harbor, intended as a first strike to eliminate American opposition, would prove a miscalculation on a par with Hitler's invasion of Russia. Hitler welcomed the Japanese surprise attack on Pearl Harbor at the time, and quickly declared war on the United States, thus, giving him justification for sinking U.S. ships crossing the north Atlantic in order to deliver supplies to Britain. This proved a benefit to President Franklin D. Roosevelt, who, up to then, had been confronted by strong isolationist opposition to war with Germany.

1943–45: The Allies victorious. Unlike the Axis, the Allies were not bound by one single formal alliance. Instead, there were agreements such as Lend-Lease, whereby the United States provided equipment to Great Britain even before it entered the war. Later, America would extend Lend-Lease to the Soviet Union, providing considerable assistance to its future Cold War enemy.

There were also a number of conferences whereby the leaders of the Allied nations planned the postwar world. These included Newfoundland in August 1941, and Casablanca in January 1943, (United States and Britain only), Teheran in November 1943, Yalta in February 1945, and Potsdam in July 1945. (By the latter point, Roosevelt had died and was replaced by Vice-President Harry S. Truman, while Churchill had been voted out in favor of Clement Atlee and the Labour Party.)

As with the Axis alliance of Germany and Italy, there was an alliance within this alliance—that of the United States and Britain. Between Roosevelt and Churchill was a strong personal bond that reflected the ultimate commonality of aims between their two nations. More strained was the relation of these leaders with Stalin. The alliance with Soviet Russia was a marriage of convenience, as all three powers faced a common enemy in Nazi Germany, but Churchill in particular never let down his guard where Stalin was concerned. (And he was right to do so, as Stalin's intelligence services were busy gathering secrets in England.)

To a much smaller extent, the United States and United Kingdom made common cause with the Chinese Nationalists, led by Chiang Kai-shek, and the Free French under General Charles de Gaulle. In neither case did these leaders speak for their entire nations. Chiang's Nationalists expended greater resources on fighting the Communists, led by Mao Tse-tung, than they did against the Japanese invaders. The Communists, who enjoyed widespread peasant support, proved able defenders, and though they would become enemies of the United States, at the time America regarded them as a useful ally against the Japanese. As for de Gaulle, who operated from London, he represented only a tiny portion of France, most of which made little effort to resist Nazi and Vichy rule.

Driving back the Axis in Europe. In Russia, the Germans got as far as the suburbs of Moscow before the winter—along with the resurgent Red Army and a defiant populace—caught up with them. Lengthy sieges at Stalingrad and Leningrad (the latter lasting more than 800 days) would spell an end to German hopes of conquest. Led by Georgi Zhukov, the Red Army gradually drove back the Germans and began the long, steady push into central Europe.

After defeating the Germans in North Africa in late 1942, the Allies invaded Sicily in July 1943, and Italy itself on September 9. This forced Mussolini to retreat to northern Italy, where he would serve as puppet ruler of a Nazi-controlled state for the remaining two years of his life. On June 6, 1944, an Allied force of some 2,700 ships and 176,000 U.S., British, Canadian, and other troops landed at Normandy, in the largest amphibious invasion in history.

By the end of 1944, Allied victory in Europe began to seem all but imminent, but a number of obstacles still stood in the way. Hitler's scientists had developed the V2 rocket, precursor of modern missiles, and Germany fired several of them against England. The Allies, meanwhile, relentlessly bombed German cities, bringing the Reich to its knees. The Battle of the Bulge in the Ardennes forest in December 1944 was the later major Axis offensive in Europe.

With the Soviets surrounding Berlin, Hitler on April 30, 1945, committed suicide in his bunker with his mistress, Eva Braun, along with propaganda minister Josef Goebbels and Goebbels's family. Two days earlier, Mussolini and his mistress, captured by Italian resistance fighters, had been shot. The Germans surrendered to the Allies on May 7. Only after the surrender did the full magnitude of the Holocaust become apparent, and for this and other crimes, those German military and political leaders who did not commit suicide would be tried before the World Court.

The defeat of Japan. In the carrier-dominated Battle of the Coral Sea in May 1942, the first naval battle in which opposing ships never caught sight of one another, neither side gained a clear victory, but the Allies won the upper hand at the Battle of Midway the following month. Later that summer, the U.S. Marines fought the Japanese at Guadalcanal in the Solomon Islands, one of the bloodiest battles of the war. Late in 1943, the Marines began a series

of assaults on Pacific islands, including the Gilbert, Marshall, Caroline, and Mariana chains. Allied forces under General Douglas MacArthur liberated the Philippines in the fall of 1944.

Early in 1945, Allied forces under Major General Curtis LeMay began dropping incendiary bombs on Japanese cities, while the Marines took the nearby islands of Iwo Jima and Okinawa. Still, the Japanese resisted, and Allied leaders contemplated a land invasion, to begin in November. The invasion, they calculated, would cost as many as 1 million American lives, with untold casualties on the among the Japanese.

Instead of invading Japan, the United States unleashed the results of the Manhattan Project, which it had begun secretly 1942. Before dropping the atomic bomb, the Allies issued one more plea for the Japanese to surrender, and when they did not, the American B-29 bomber *Enola Gay* dropped a bomb on the city of Hiroshima. Despite the devastation wrought by this, the first use of a nuclear weapon in warfare, the Japanese still refused to surrender. On August 9, the United States dropped a second bomb, this one on Nagasaki. At this point, Hirohito urged the nation's leaders to surrender. Tojo and several others committed suicide, and on September 2, 1945, Japanese representatives formally surrendered.

A War of Information, Images, and Ideas

The Manhattan Project was the most dramatic expression of a theme that ran through the entire conflict, that ideas and information often contribute as much to a successful military effort as do troops and weapons. Though the First World War brought airplanes into widespread use, along with tanks, and resulted in the popularization of radio soon afterward, the Second World War saw the first true marriage of science and defense to yield the military-industrial complex familiar today. Its legacy is evident in the many technological innovations that were either introduced during its course, or very soon after the fighting ended. In addition to nuclear power and the missile, these include radar, computers, jet engines, and television.

The war also introduced modern concepts of covert and special operations, on the part of the OSS, the British Special Operations Executive (SOE), military intelligence units, and special warfare units that included the Rangers and the precursors to the Navy SEALS of today. The Germans had their spies as well, some of whom even managed to infiltrate the United States, but their efforts in this regard were never as successful as those of the Allies.

Cryptology. In the cryptologic war, the Allies were the unquestioned victors. Perhaps the single greatest intelligence success of the war was the British deciphering of the Germans' secret system of communications. Early in the war, British and Polish intelligence officers obtained a German Enigma cipher machine, to which a team of mathematicians at Bletchley Park applied their expertise. The result was Ultra, the British system for reading the German ciphers.

Thanks to Ultra, the British knew many of the targets in advance during the Battle of Britain. In north Africa in 1942, Ultra helped Field Marshal Bernard Montgomery predict Rommel's actions. So vital was the Ultra secret that the British used it with the utmost of caution, careful not to act to often or too quickly on information it revealed for fear that this might tip off the Germans. Only in the 1970s did the world learn of the Ultra secret.

American successes included the breaking of the Japanese RED cipher by the U.S. Navy, and the PURPLE cipher by the U.S. Army Signal Intelligence Service prior to the war. During the war, the navy proved more successful at breaking the ciphers of its counterpart than did the army. Also notable was the American use of codetalkers transmitting enciphered messages in the Navajo Indian language, which made their transmissions indecipherable to the Japanese. Neither the Japanese nor the Germans scored any major cryptologic victory against the Allies.

Deception, secrets, and covert operations. The Allied invasion of Italy was accompanied by a number of behind-the-scenes moves. Just before the invasion of Sicily, British naval intelligence obtained the body of a man who had recently died, and arranged for his body—clad in the uniform of a major in the Royal Marines—to wash up on a shore in Spain. On his person were documents laying out a British plan for an imminent invasion of the Balkans, information the British knew the Germans (who had numerous agents in Spain) would acquire. The ruse, known as Operation Mincemeat (subject of the 1953 film *The Man Who Never Was*) left the Germans unprepared for the subsequent invasion.

The surrender of most of Italy by Marshal Pietro Badoglio appears to have been the result of behind-the-scenes talks with the Allies. During the moments of turmoil in the capital as Mussolini's government was overthrown, a British intelligence officer provided Badoglio with a safe haven. In 1945, Allen Dulles—future director of the CIA—secretly negotiated with SS General Karl Wolff for the surrender of all German forces in Italy.

Another deception campaign, known as Bodyguard, preceded the Normandy invasion of June 1944. Using German agents in England who had been turned by British intelligence, the Allies conducted an elaborate campaign designed to convince the Germans that they were attacking anywhere but Normandy. Radio transmission from Scotland seemed to indicate a thrust toward Norway, while the appearance of Montgomery near Gibraltar suggested an invasion through Spain. (In fact "Montgomery" was actually a British actor who resembled the general.)

The Normandy deception included the creation an entire unit, the First U.S. Army Group (FUSAG), from thin

air. FUSAG, which was supposed to be landing at Calais rather than Normandy, had a putative commander in General George S. Patton, fresh from victories in North Africa and Italy. Large tent encampments created the illusion of massive troop strength, while fake tanks, landing craft, and other equipment gave indications that the Allies were gearing up for a major operation. So, too, did radio communications from Patton's headquarters, as well as a heavy Allied bombing campaign over Calais in the days leading up to June 6. The ploy succeed in diverting 19 German divisions from Normandy.

The race to develop an atomic bomb involved several covert operations, including British sabotage directed against Nazi weapons materials in Norway, as well as an intelligence-gathering operation known as Alsos. The name was chosen by Major General Leslie Groves, who oversaw the Manhattan Project, because *alsos* is Greek for "grove." Members of the Alsos team, which included both U.S. Army and Navy personnel, scoured research laboratories in Germany, Italy, France, and Belgium for information on Axis bomb-making efforts.

Propaganda. At the simplest level of ideas, propaganda—though a feature of wars since the beginning of history—played a particularly significant role in the Second World War. Its importance to the Nazis is symbolized by the fact that in his final hours, Hitler had Goebbels beside him. Goebbels, who like Mussolini was a former Communist, had powerful instincts for making appeals to the populace, using all available media, including print, radio, and film. (The Nazis even conducted early experiments with television.)

Films by Leni Riefenstahl in the 1930s romanticized the myth of Aryan superiority, while cruder propaganda from Goebbels' office excited hatred toward Jews. During the war, Axis powers on both sides of the world made considerable use of radio through broadcasters such as Lord Haw Haw (a.k.a. William Joyce), Axis Sally (Mildred Gillars, an American), and a number of Asian females collectively dubbed "Tokyo Rose" by U.S. forces. The Allies conducted a propaganda war of their own, through radio broadcasts and the efforts of the U.S. Office of War Information and the Voice of America.

FURTHER READING:

BOOKS:

Breuer, William B. *Undercover Tales of World War II.* New York: J. Wiley, 1999.

Farago, Ladislas. *The Game of the Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II.* City: Publisher, 1971.

Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage.* New York: Random House, 2001.

Shirer, William. *The Rise and Fall of the Third Reich.* New York: Simon and Schuster, 1960.

West, Nigel. *A Thread of Deceit: Espionage Myths of World War II.* New York: Random House, 1985.

SEE ALSO

Army Security Agency
Cameras
Cold War (1945–1950), The start of the Atomic Age
COMINT (Communications Intelligence)
Cryptology, History
Enigma
FBI (United States Federal Bureau of Investigation)
FISH (German Geheimschreiber *Cipher Machine*
French Underground during World War II, Communication and Codes
Germany, Intelligence and Security
Gestapo
Italy, Intelligence and Security
Japan, Intelligence and Security
Korean War
OSS (United States Office of Strategic Services)
Pearl Harbor, Japanese Attack on
RADAR
Red Orchestra
Room 40
SOE (Special Operations Executive)
Soviet Union (USSR), Intelligence and Security
Special Relationship: Technology Sharing between the Intelligence Agencies of the United States and United Kingdom
Truman Administration (1945–1953), United States National Security Policy
Ultra, Operation
United Kingdom, Intelligence and Security
Vietnam War
World War I
World War II, The Surrender of the Italian Army
World War II, United States Breaking of Japanese Naval Codes
World War II: Allied Invasion of Sicily and "The Man Who Never Was"

World War II: Allied Invasion of Sicily and "The Man Who Never Was"

ADRIENNE WILMOTH LERNER

As the World War II Allied campaign in North Africa drew to a close, Allied command turned its attention to its next major objective, an invasion of Europe. From their position in North Africa, with the aid of their fleet in the Atlantic and Mediterranean, the next logical targets for the Allies were German defenses on the Italian island of Sicily.

However, rough terrain and solid German land and air defenses would make a direct assault on the island costly, and potentially disastrous. As the German command expected the Allies to attack Sicily, Allied intelligence was charged with devising a plan to feed misinformation to the Germans, causing them to believe that Allied forces were massing to invade Europe via Greece or the Balkans. The plot became known as "Operation Mincemeat," or "the man who never was."

Two British intelligence agents, Ewen Montagu and Sir Archibald Cholmondley, members of the XX "double cross" intelligence committee, proposed to use a dead body, dressed as a military courier, to slip false information about Allied battle plans to the German intelligence service, the Abwehr. The two men convinced Allied command that, with enough attention to the ruse courier's body, uniform, placement, and personal effects, Abwehr agents were sure to believe the validity of any information the courier carried. The team was given less than three months to carry out the "man who never was" operation.

Montague first located a suitable body, that of man in his 30s who had died of pneumonia. Since the team planned to deliver the body by sea, making it look as though the victim washed ashore after a plane crash, the similarity of the pathology of pneumonia and drowning was highly convenient. After gaining the consent of the dead man's family, the body was kept in cold storage while a the XX intelligence team went to work on "Operation Mincemeat," creating a false identity and personal effects for their mystery soldier.

The XX team dressed the body in a Royal Marine uniform, and stuffed his pockets with typical soldier accoutrements. Because the corpse's false identity would have to appear in public casualty noticed printed in the newspapers, the corpse was given the most common name on British military rolls, (acting Capt.) William Martin. Montague and Cholmondley convinced their secretary to write letters to Martin, posing as his fiancée. They included her picture in "Mincemeat's" pockets.

After producing the false documents and private communications between field generals that were added to Martin's attaché case, the body was ready to transport, via submarine, to the Spanish coast. The team chose the location because of the plethora of German agents working in the region. In addition, it gave the illusion that the courier was trying to avoid travel over hostile territory. The body was released into the water off the coast of Spain on April 19, 1943. A fishing boat retrieved the remains of the "man who never was," and reported the find to German agents.

Immediately, British intelligence published William Martin's name on public casualty lists, with the explanation of missing, presumed dead in air accident. Intelligence officers knew that Abwehr agents would check public records to confirm the man's identity. To further the deception, the XX team held a mock funeral for Martin back in England, complete with flowers and a grieving fiancée.

British military intelligence cryptanalysis staff at Bletchley Park monitored German Enigma encoded messages almost in real time. Intercepts indicated that Martin had been found and that the Abwehr had located the misinformation planted on the corpse. Remarkably, within weeks, intercepts reveled that the German High Command had distributed the information to Generals in the Mediterranean. On May 12, 1943, the Germans moved thousands of troops, airplanes, and weaponry from Sicily to fortify defenses in Sardinia and Greece, where they presumed Allied forces were going to invade.

Allied forces invaded Sicily on the morning of July 9. Operation Mincemeat succeeded in weakening German outposts on the island, and allowed the Allies to sweep ashore with astonishing surprise. Though fighting persisted on the island for a month, the clever deception of the "man who never was," whose true identity has never been revealed, greatly reduced the human cost of the invasion for Allied forces. Sicily fell to Allied control on August 17, 1943.

FURTHER READING:

BOOKS:

Hinsley, F. H. *British Intelligence in the Second World War.* Cambridge: Cambridge University Press, 1988.

Montagu, Ewen. *Man Who Never Was.* London: Globe Pequot Press, 1997.

SEE ALSO

Bletchley Park
Codes and Ciphers
Codes, Fast and Scalable Scientific Computation
Enigma
OSS (United States Office of Strategic Services
Poland, Intelligence and Security
Ultra, Operation
United Kingdom, Intelligence and Security

World War II, The Surrender of the Italian Army

JUDSON KNIGHT

The Allied victory in Italy, beginning with the surrender of the Italian government in 1943 and continuing through the conclusion of the war in Europe two years later, was as much a triumph of intelligence, psychological warfare,

and special operations as it was a victory of military might. Among the players in this undertaking were the British Special Operations Executive (SOE), the American Office of Strategic Services (OSS), various units engaged in psychological warfare, and the Italian partisans who fought to regain control of their country.

Badoglio's capitulation. By 1943, popular sentiment had long since turned against the Fascist government of Benito Mussolini, but the heavy presence of German troops made the Italians virtual prisoners to the Axis. Faced with this quandary, Prime Minister Pietro Badoglio established clandestine communications with the Allies by diplomatic channels. He thus paved the way for the overthrow of Mussolini on July 25, after which the dictator was arrested. The Allies landed at the beginning of September.

The fact that the fighting in Italy would last until the conclusion of the war—the longest single campaign waged by British and American forces—serves to indicate that matters did not go smoothly even after Badoglio's surrender. A major factor in this was the Germans' resolve to hold on to the northern portion of the country. There, Mussolini (rescued in a daring German airborne raid on September 12) ruled a puppet government, but the real power lay in the hands of the Nazis.

The Allied effort. To counter the Nazis' hold on northern Italy, the Allies undertook a number of operations to support the military forces. The latter consisted of the 15th Army Group, commanded by Britain's General Sir Harold R. L. G. Alexander, which included General Bernard Montgomery's British 8th Army, General George S. Patton's U.S. 7th Army, and Lieutenant General Mark C. Clark's 5th U.S. Army. Patton and Montgomery led Operation Husky, the invasion of Sicily in June 1943, while Clark and Montgomery made the first assault on the Italian peninsula three months later.

Assisting this military effort were psychological warfare units of the U.S. 5th Army and the British 8th Army. Klaus Mann, a German American with the 5th Army, designed leaflets intended for the German soldiers. At the same time, OSS was heavily involved behind the scenes. Leading OSS operations was Max Corvo, a Sicilian American who, as a young army private in 1942, had taken a three-day pass to Washington, D.C., and presented a plan for the subversion in Sicily. He soon received a transfer to OSS, and from 1943 to early 1945, Corvo, still in his mid-twenties, ran OSS Italian operations.

At the same time, the Office of Naval Intelligence undertook its own efforts, including one of the most famous (or infamous) aspects of the covert war in Italy: the release of Mafia chieftain "Lucky" Luciano from a Stateside prison to conduct advance work in Sicily. This effectively shut out Corvo who, knowing the Mafia well from his childhood, refused to work with gangsters. Corvo would later be replaced by James Jesus Angleton, destined to become a major figure in the postwar Central Intelligence Agency. Angleton, a hardline anti-Communist even then, wished to avoid dealing with the Left—a difficult task in a country that had the largest Communist Party of any non-Communist country in Europe. Instead, Angleton ended up working with Masons, syndicalists (non-Communist leftists associated with anarchism), and disaffected Fascists.

The partisans. In the shadow war against the Germans, few elements did as much to undermine Nazi power as the Italian partisans, who worked closely with the OSS and the SOE. These Italian irregulars tied up seven German divisions, and forced two of these to surrender, sapping German strength in Italy. With the help of OSS, partisans infiltrated German lines via submarine. Partisan agents such as Mino Farneti set up secret radio communications and arranged parachute drops of weapons to enable a counterattack by partisan forces in the north.

Another partisan aided the escape of five Allied generals who had been captured by the Nazis. In September 1944, a team led by this same operative intercepted and shot a German major traveling by sidecar. In his briefcase they found detailed plans of the Germans' defenses for the eastern half of the Gothic Line. Another partisan smuggled a set of plans for the western half in the sole of his boots, and delivered these to OSS operatives in Siena. Thanks to these plans, the Allied force broke through the Gothic Line on September 17.

■ FURTHER READING:

BOOKS:

Chalou, George C. *The Secrets of War: The Office of Strategic Services in World War II.* Washington, D.C.: National Archives and Records Administration, 1992.

Corvo, Max. *The O.S.S. in Italy, 1942–1945: A Personal Memoir.* New York: Praeger, 1990.

Dulles, Allen. *The Secret Surrender.* New York: Harper and Row, 1966.

ELECTRONIC:

Prosser, Frank, and Herb Friedman. "Organization of the United States Propaganda Effort during World War II." Psychological Warfare and Aerial Propaganda Leaflets. <http://psywar.psyborg.co.uk/> (April 7, 2003).

Tomkins, Peter. "The OSS and Italian Partisans in World War II." Center for the Study of Intelligence, Central Intelligence Agency. <http://www.cia.gov/csi/studies/spring98/OSS.html> (April 7, 2003).

SEE ALSO

OSS (United States Office of Strategic Services)
Propaganda, Uses and Psychology
SOE (Special Operations Executive)
World War II

World War II, United States Breaking of Japanese Naval Codes

MICHAEL J. O'NEAL

On December 7, 1941, Japanese military forces attacked the United States naval fleet anchored at Pearl Harbor on the Hawaiian island of Oahu. The surprise attack was devastating to the U.S. Navy. Nearly every American plane on Oahu was destroyed; three cruisers, three destroyers, and eight battleships were severely damaged, and two battleships, the *Oklahoma* and the *Arizona* were destroyed; over 2,300 U.S. servicemen lost their lives. In the weeks and months that followed, fears ran deep among shocked Americans that Japan had the ability to launch an invasion on the West Coast of the United States. At the very least, it was feared that the Japanese Navy, facing only the remnants of a tattered American fleet, could effectively control the Pacific Ocean, cutting the United States off from vital resources and shipping lanes.

Over the next three and a half years, in a series of fierce sea and island battles, American forces managed to push the Japanese empire back to its own shores. They were able to do so not only through courage and resolve, but also through the efforts of hundreds of men and women who labored in secrecy, many of them twelve hours a day, seven days a week, cracking the codes that Japanese forces used to transmit messages. Without the information revealed by breaking these codes, the U.S. military could never have countered Japanese offensives throughout the vast expanse of the Pacific, for they would never have known where the Japanese intended to strike next.

Early code-breaking efforts. Even before World War I, the United States had been regularly deciphering coded messages sent by foreign diplomats. On the basis of decoded diplomatic messages, for example, the United States and Great Britain knew what arms limitations the Japanese would accept in the peace talks following the war, and negotiators bargained accordingly. The effort to break Japanese diplomatic codes continued into the 1920s and 1930s under the direction of William Friedman, a Russian immigrant who was appointed chief cryptanalyst of the Army Signal Intelligence Service (SIS) in 1922. In the late 1930s, SIS cryptanalysts succeeding in breaking the Purple code, also designated AN-1, which was the principal cipher Japan used to send diplomatic messages. (While the terms code and cipher are often used interchangeably, a code is a substitution of one character or string of characters for another; reading a cipher, however, usually requires application of some kind of mathematical operation specified by a cipher key; a simple cipher, for example, might require the decoder to subtract a designated value from a string of numbers to arrive at the true string of numbers that encodes a letter, word, or phrase.)

JN-25. On June 1, 1939, the Japanese introduced what American cryptanalysts called JN– 25. JN means simply Japanese Navy, and JN–25, consisting eventually of about 33,000 words, phrases, and letters, was the primary code the Japanese used to send military, as opposed to diplomatic, messages. After Pearl Harbor, U.S. intelligence efforts focused on cracking JN–25. Leading the effort, code-named Magic, was the U.S. Navy's Combat Intelligence Unit, called OP–20–G and consisting of 738 naval personnel. The unit, housed in the basement of the 14th Naval District Administration at Pearl Harbor, was under the command of Commodore John Rochefort, who combined fluency in Japanese with single-minded dedication to the task. Using complex mathematical analysis, IBM punch-card tabulating machines, and a cipher machine, Friedman had developed the ECM Mark III, the unit was able to crack most of the code by January 1942. The blanket name given to any information gained by deciphering JN–25 was Ultra, a word borrowed from British codebreaking efforts and stamped at the top of all deciphered messages.

The Combat Intelligence Unit worked tirelessly, but the unit had some help from the Japanese themselves. For example, messages, primarily radio transmissions, often began with such stylized phrases as "I have the honor to inform your excellency" and with the names of ships, locations, commanders, the time and date, and similar repeated information that could be easily verified; many referred to military and other officials by formal, stylized titles. These weaknesses, combined with the fact that the Japanese introduced changes to the code only every three to six months, gave American cryptanalysts a toehold into the code. Soon they were able to read the code, which consisted of strings of five digits. Thus, for example, the string 97850 meant submarine, although because JN–25 was really a cipher, the cryptanalyst had to subtract a value from the string of digits to arrive at the correct meaning. Making this task somewhat easier for Americans, the Japanese changed their cipher key infrequently.

Putting the code to use. Armed with the ability to read Japanese operational messages, the U.S. Navy was able turn back the Japanese advance in the Pacific in mid-1942. In April of that year, decrypted messages revealed that Japanese forces were preparing for an assault on Port Moresby, an Australian base in New Guinea, on May 7. In response, U.S. Admiral Chester Nimitz moved his fleet into the Coral Sea between New Guinea and Australia. While the ensuing two-day Battle of Coral Sea was considered a draw, U.S. forces inflicted enough damage on the

Japanese navy to force it to withdraw, giving the United States and Australia time to reinforce Allied defenses in New Guinea.

Perhaps the most dramatic success that resulted from breaking the Japanese naval code was the Battle of Midway in June 1942. The plan of Japanese commander Admiral Isoroku Yamamoto was to assemble an aircraft carrier task force, launch a diversionary raid off the Aleutian Islands, and lure the U.S. Navy to Midway Island and into a decisive battle that would destroy what remained of the American fleet after Pearl Harbor. From decrypted messages, U.S. naval commanders knew the general outlines of the plan, even the timetable. The messages, however, did not say where the Japanese intended to strike; the target was simply designated "AF." It was Rochefort who proposed a ruse to determine what AF stood for. Suspecting that it was Midway Island, he arranged for American forces on the island to send out a radio message saying that they were running short of fresh water. Rochefort and his group waited anxiously to see if Japan would take the bait. Finally, codebreakers intercepted a Japanese message: AF was running short of fresh water. Knowing that the assault was to come at Midway, the U.S. Navy was ready. On June 4, 1942, after a fierce three-day battle, U.S. pilots sank all four Japanese aircraft carriers in Yamamoto's task force, effectively turning the tide in the Pacific. Later, in an unintended breach of wartime security, the *Chicago Tribune* published a story revealing that the navy had known about Japanese intentions in advance, in effect revealing that JN–25 had been broken. The Japanese never found out about the article.

In a postscript to the Battle of Midway, Admiral Yamamoto lost his life as a result of a decrypted message. Codebreakers learned that the admiral was scheduled to inspect a naval base on Bougainville in the Solomon Islands on April 18, 1943. Some U.S. policy makers were hesitant to use this information for fear that doing so would tip off the Japanese that their codes had been broken. Nevertheless, the decision was made to assassinate Yamamoto. That morning, eighteen P–38 fighters left their base at Guadalcanal at the other end of the Solomon chain and arrived at Bougainville just as Yamamoto's plane was making its approach. The admiral was killed in the attack, depriving Japan of its most experienced and accomplished admiral and sapping Japanese morale. To maintain the fiction that the fighters had arrived by chance, the air force flew other patrols in the area, both before and after the attack. The Japanese did not change JN–25, and for the remainder of the war, U.S. intelligence intercepted and read thousands of Japanese messages.

FURTHER READING:

BOOKS:

Benson, Robert Louis. *A History of U.S. Communications Intelligence During World War II: Policy and Administration.* Washington, D.C.: Center for Cryptologic History, National Security Agency, 1997.

Farago, Ladislas. *The Broken Seal.* New York: Random House, 1967.

Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage.* New York: Random House, 2001.

Winton, John. *Ultra in the Pacific: How Breaking Japanese Codes & Cyphers Affected Naval Operations Against Japan: 1941–1945.* London: Leo Cooper, 1993.

ELECTRONIC:

"Cryptography in the Modern Age." <http://www.cnn.com/SPECIALS/2001/nsa/stories/crypto.history/> (January 9, 2003).

Singh, Simon. "US Codebreakers in World War II." <http://www.vectorsite.net/ttcode7.html> (January 9, 2003).

SEE ALSO

Cipher Machines
Codes and Ciphers
Cryptology, History
Pearl Harbor, Japanese Attack on
Purple Machine
World War II

X-ray Scanners.

SEE *Scanning Technologies.*

Zimmermann Telegram.

SEE *United States Intelligence, History.*

Zoonoses

BRIAN HOYLE

Zoonoses are diseases of microbiological origin that can be transmitted from animals to people. The causes of the diseases can be bacteria, viruses, parasites, and fungi.

Some zoonotic diseases are identified as potential diseases (e.g., Tularemia) could be exploited by bioterrorists to cause death—including death or contamination of livestock—and widespread economic damage. As of May 2003, the best scientific evidence available suggested that the cornonavirus responsible for Severe Acute Respiratory Syndrome (SARS) was originally transmitted from animal hosts.

Zoonoses are relevant for humans because of their species-jumping ability. Because many of the causative microbial agents are resident in domestic animals and birds, agricultural workers and those in food processing plants are at risk. From a research standpoint, zoonotic

diseases are interesting as they result from organisms that can live in a host innocuously while producing disease upon entry into a different host environment.

Humans can develop zoonotic diseases in different ways, depending upon the microorganism. Entry through a cut in the skin can occur with some bacteria. Inhalation of bacteria, viruses, and fungi is also a common method of transmission. As well, the ingestion of improperly cooked food or inadequately treated water that has been contaminated with the fecal material from animals or birds present another route of disease transmission.

A classic historical example of a zoonotic disease is yellow fever. The construction of the Panama Canal took humans into the previously unexplored regions of the Central American jungle.

A number of bacterial zoonotic diseases are known. A few examples are Tularemia, which is caused by *Francisella tulerensis*, Leptospirosis (*Leptospiras spp.*), Lyme disease (*Borrelia burgdorferi*), Chlaydiosis (*Chlamydia psittaci*), Salmonellosis (*Salmonella spp.*), Brucellosis (*Brucella melitensis, suis,* and *abortus*), Q-fever (*Coxiella burnetti*), and Campylobacteriosis (*Campylobacter jejuni*).

Zoonoses produced by fungi, and the organism responsible, include Aspergillosis (*Aspergillus fumigatus*). Well-known viral zoonoses include rabies and encephalitis. The microorganisms called Chlamydia cause a pneumonia-like disease called psittacosis.

Within the past two decades two protozoan zoonoses have definitely emerged. These are Giardia (also commonly known as "beaver fever"), which is caused by *Giardia lamblia,* and Cryptosporidium, which is caused by *Cryptosporidium parvum*. These protozoans reside in many vertebrates, particularly those associated with wilderness areas. The increasing encroachment of human habitations with wilderness is bringing the animals, and their resident microbial flora, into closer contact with people.

Similarly, human encroachment is thought to be the cause for the emergence of devastatingly fatal viral hemorrhagic fevers, such as Ebola and Rift Valley fever. While the origin of these agents is not definitively known, zoonotic transmission is virtually assumed.

Outbreaks of hoof and mouth disease among cattle and sheep in the United Kingdom (the latest being in 2001) has established an as yet unproven, but compelling, zoonotic link between these animals and humans, involving the disease causing entities known as prions. While the story is not fully resolved, the current evidence supports the transmission of the prion agent of mad cow disease to humans, where the similar brain degeneration disease is known as Creutzfeld-Jacob disease.

The increasing incidence of these and other zoonotic diseases has been linked to the increased ease of global travel. Microorganisms are more globally portable than ever before. This, combined with the innate ability of microbes to adapt to new environments, has created new combinations of microorganism and susceptible human populations.

FURTHER READING:

BOOKS:

Chin, J. "Tularemia." *Control of Communicable Diseases Manual.* Washington, DC: American Public Health Association, 2000.

ELECTRONIC:

World Health Organization. WHO Fact Sheets (May, 2003) <http://www.who.int/health-topics/zoonoses.htm> (May 12, 2003).

SEE ALSO

Bioterrorism, Protective Measures
Infectious Disease, Threats to Security

This page intentionally left blank

Glossary

A Compendium of Common Acronyms and Terms

17 November Organization Revolutionary Organization 17 November (17 November).

AAIA Aden-Abyan Islamic Army.

AAMVA American Association for Motor Vehicle Administration.

ABB Alex Boncayao Brigade.

ABI Airborne Broadcast Intelligence.

ABM Treaty The Antiballistic Missile (ABM) Treaty was signed by the United States and the Soviet Union (U.S.S.R.) in 1972. The treaty was one of two treaties produced by the first series of Strategic Arms Limitation Talks (SALT I) between the two countries; the other was an interim agreement limiting offensive nuclear weapons.

ABMDA Army Ballistic Missile Defense Agency.

ABMT The focus of the Advanced Biomedical Technologies Program (ABMT) is to apply techniques in robotics, virtual reality, three-dimensional visualization, telesurgery, microelectromechanical systems (MEMS), informatics and multi-media simulation to producing products for the care of wounded personnel on the front lines of war.

Abwehr The German military intelligence organization from 1866 to 1944.

ACCES Advance Cryptologic Carry-on Exploitation System.

Accommodation Address An address used by intermediates to transfer messages.

ACDBU Automated Counterdrug Database Update.

ACIPS Acoustic Intelligence Processing System.

Acoustic bullets Scalable low-frequency (10-Hz) sound pulses sent over distances of hundreds of yards, scalable in intensity from painful to lethal.

Acoustic intelligence Information derived from audio sources.

Acoustics The study of the creation and propagation of mechanical vibration causing sound.

Active SONAR Mode of echo location by sending a signal and detecting the returning echo.

ADARS Airborne Digital Audio Recording System.

ADC Analog to digital conversion.

ADF Allied Democratic Forces.

ADFGX cipher A code that applies the Polybius square in such a way that the letters *A, D, F, G,* and *X* take the place of numbers for the rows and columns. Some versions, known as the ADFGVX cipher, use the letter *V* to provide additional rows and columns, thus making possible the inclusion of the ten numerals along with the letters of the alphabet.

ADIO Australian Defense Intelligence Organization.

ADSD Australian Defense Signals Directorate.

Advanced Encrytion Standard A cipher algorithm standardized for use by U.S. government agencies and departments.

AEC Atomic Energy Commission.

AEOS Advanced Electro-Optical System.

Aerostat An unmanned, aerodynamically shaped blimp tethered to the ground by a single cable.

AES The CryptoAPI algorithm name for the Advanced Encryption Standard algorithm.

AFI Air Force Intelligence.

AFINTNET Air Force Intelligence Network.

AFIP Armed Forces Institute of Pathology.

AFIS Automated fingerprint identification systems.

Aflatoxin Aflatoxins belong to a group of toxins called mycotoxins, which are derived from fungi.

AFOSI The Air Force Office of Special Investigations is the principal investigative service of the United States Air Force.

AFSA Armed Forces Security Agency, a forerunner of the National Security Agency.

Agent A person hired or recruited by an intelligence agency to do its bidding. Compare with *operative.*

Agent H blister agent Mustard bis-(2-chloroethyl)sulfide.

Agent L Lewisite: dichloro(2-chlorovinyl) arsine.

Agent of influence A person who does not directly work for an intelligence agency, but willingly acts on its behalf to influence public or political opinion.

Agent orange A defoliant; that is, a chemical that kills plants and causes the leaves to fall off the dying plants.

Agent provocateur An operative or agent who infiltrates a group or organization with the purpose of inciting its members to self-destructive acts.

Agent Q Sesquimustard, 1,2-bis-(2-chloroethylthio)ethane.

Agent T Agent T bis-(2-chloroethylthio ethyl)ether (potential mustard agent additive).

Agent-in-place An employee of one intelligence agency who, of his or her own initiative, offers services to a rival or enemy agency. The agent-in-place continues to work for the first agency, and feed information to the second one.

AHFEWS Army HF Electronic Warfare System AN/TLQ-33.

AI Army Intelligence.

AIAI Al-Ittihad al-Islami.

AIIB Anti-Imperialist International Brigade.

Air Force Office of Special Investigations (AFOSI) The principal investigative service of thee United States Air Force.

Air marshal United States air marshals are the first police force of the federal government created solely to protect against air terrorism.

Air plume A layer of warm air that immediately surrounds a person's body. It has also been referred to as a human thermal plume.

AIRES Advanced Imagery Reqs & Exploitation System.

AIRTAPS Aerial Imagery Reconnaissance Tracking and Plotting System.

Aleph Aum Supreme Truth (Aum) Aum Shinrikyo, Aleph.

ALG class key exchange The CryptoAPI algorithm class for key exchange algorithms.

Algorithm A method for solving a mathematical problem by using a finite number of computations, usually involving repetition of certain operations or steps. Frequently used in computer science.

ALIR Army for the Liberation of Rwanda.

Al-Qaeda Responsible for the September 11, 2001, terrorist attacks upon the United States, Al-Qaeda (also known as Al-Qaida) was established by Osama bin Ladin (also spelled Usama Bin Ladin or Osama bin Laden) in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Al-Qaeda helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Al-Qaeda's current goal is to establish a pan-Islamic caliphate throughout the world and has declared the United States to be an enemy to be attacked by terrorist actions.

AM-band Amplitude Modulated (AM) radio carrier frequencies 535–1605 kHz assigned by the FCC in 10 kHz intervals.

AM-band (maritime and aircraft navigation frequencies) Amplitude Modulated (AM) radio carrier frequencies 30 to 535 kHz.

AMU Atomic mass units.

ANNULET Cryptologic maintenance system.

ANO Abu Nidal Organization.

ANSI American National Standards Institute.

ANSIR FBI Awareness of National Security Issues and Response Program.

Anthrax A disease that is caused by the bacterium *Bacillus anthracis*. The bacterium can enter the body via a wound in the skin (cutaneous anthrax), via contaminated food or liquid (gastrointestinal anthrax), or can be inhaled (inhalation anthrax).

Antibiotics Agents that kill bacteria. Antibiotics act only on bacteria and are not effective against viruses.

Antivirals Compounds that are used to prevent or treat viral infections via the disruption of an infectious mechanism used by the virus.

Anvil Automated Target Recognition on Multi-Spectral Imagery.

APF Alliance of Palestinian Forces.

APIS The Advance Passenger Information System (APIS) is an electronic database system that stores information about airline travelers. The system, operated by the United States Customs Service, the Immigration and Naturalization Service (INS), and the Federal Aviation Administration (FAA), provides searchable biographical and security information on air travelers entering the United States from a foreign destination.

Apogee An orbital position were a satellite is farthest from Earth.

Apogee Kick Motor (AKM) Satellite rockets that boost a satellite from a temporary orbit to a geostationary (GEO) orbit.

APS Advanced Photon Source.

ARAC The Atmospheric Release Advisory Capability (ARAC) is an effort through which the United States Department of Energy (DOE) monitors and predicts the release of hazardous materials into the atmosphere.

Area 51 The popular name of a secret military facility at Groom Lake, Nevada, approximately ninety miles north of Las Vegas. The six-by-ten mile rectangular air base lies within the Switzerland-sized boundaries of Nellis Air Force Base, and has served as a testing ground for "black budget" (top-secret) military prototype aircraft since the mid-1950s. Area 51 is also a well-known folk symbol of an alleged, but scientifically improbable, government conspiracy to cover up information on UFOs and extraterrestrial life.

AREAS Airborne Reconnaissance Evaluation and Analysis System.

ARGUS Army intelligence database.

ARPANet Early DARPA program that led to the development of the Internet.

Array A large group of hydrophones, usually regularly spaced, forming a SONAR net.

ASA The Army Security Agency (ASA) provided the United States Army with signal intelligence and security information from 1945 to 1976.

ASARS Advanced Synthetic Aperture Radar System.

ASAS All Source Analysis System.

ASCI Accelerated Strategic Computing Initiative.

ASG Abu Sayyaf Group.

ASIO Australian Security Intelligence Organization.

ASIS Australian Secret Intelligence Service.

Assassination A sudden, usually unexpected act of murder committed for impersonal reasons, typically with a political or military leader as its target.

Assay A determination of an amount of a particular compound in a sample.

Assessment Evaluating the potential value of an agent or source.

Asset Agents, sympathizers, or supporters that intelligence agencies can exploit to complete mission objectives.

ASTECS Advanced Submarine Tactical ESM Combat System.

Asymmetric warfare In contrast to traditional warfare or "linear warfare," asymmetric warfare refers to operations that do not rely on masses of troops or munitions to destroy and/or control an enemy. Asymmetric warfare most commonly refers to warfare between opponents not evenly matched where the smaller or weaker force must exploit geography, timing, surprise, or specific vulnerabilities of the larger and stronger enemy force to achieve victory.

ATARS Advanced Tactical Reconnaissance Airborne System.

ATF In accordance with the Homeland Security Act of 2002, on January 24, 2003, the Bureau of Alcohol, Tobacco, and Firearms (ATF or BATF) was transferred from the Department of the Treasury to the Department of Justice. There it became the Bureau of Alcohol, Tobacco, Firearms, and Explosives, but retained the initials ATF.

ATI Air technical intelligence, or the gathering of intelligence regarding aircraft—as opposed to aerial surveillance or reconnaissance, which is intelligence gathered *using* aircraft. In some cases, aerial operations may be used to gather ATI.

ATR Automatic/Aided Target Recognition.

AUC United Self-Defense Forces/Group of Colombia (AUC).

Audio amplifier Electronic devices that increase the power of an electrical signal whose vibrations are confined to the audio frequency range—the range that can be perceived by the human ear.

Aum Shinrikyo, Aleph Aum Supreme Truth (Aum) Aum Shinrikyo, Aleph.

AUV An autonomous underwater vehicle, or small, submarine-like robot.

AVA Anthrax vaccine adsorbed.

AVS Airborne Video Surveillance.

B-2 The United States Air Force B-2 stealth technology low-observable, strategic, long-range bomber.

Bacillus anthracis The bacterium that causes anthrax.

Back door An unadvertised portal or route into a secure system.

Background Investigation Investigation of individuals who require a security clearance in working with classified documents.

Bagman An agent who acts as a paymaster to spies or makes bribes.

Ballistic fingerprint The unique pattern of markings left by a specific firearm on ammunition as it is discharged.

Ballistic missiles Any missile that lofts an explosive payload, which descends to its target as a ballistic projectile—that is, solely under the influence of gravity and air resistance—is a ballistic missile. Missiles that do not deliver a free-falling payload, such as engine powered cruise missiles (which fly to their targets as robotic airplanes), are not "ballistic."

Ballistic transport Movement of a carrier through a semiconductor without collisions, resulting in extraordinary electrical properties.

Ballistics The study of projectile motion, or the motion of objects that have been thrown, shot, or launched. In the context of forensic science, the term usually involves the study of ammunition and firearms.

Bandwidth Transponder frequency rangecapacity (generally given in MHz).

Barbiturate A class of drugs with sedative and hypnotic activities.

Barnacle The codename for a specific program within the Special Naval Collection Program (SNCP).

Barrel (of oil) The traditional unit of measure by which crude oil is bought and sold on the world market. One barrel of oil is equivalent to 159 liters (42 U.S. gallons).

Baseline In triangulation, the measured and known side of a triangle.

Bathymetric map Maps that depict the ocean (sea) depth depending on geographical coordinates, just as topographic maps represent the altitude of Earth's surface in different geographic points.

BCIS U.S. Department of Homeland Security, Bureau of Citizenship and Immigration Services.

BDA Bomb damage assessment.

BEADS Biodetection Enabling Analyte Delivery System.

BEARTRAP Acoustic data collection and processing.

Belly buster hand drill The "belly buster" hand-crank drill served as an aid to audio surveillance efforts by the United States Central Intelligence Agency (CIA) during the 1950s and 1960s. Designed to drill holes into masonry, the device made it possible to implant audio devices for covert listening.

BEP United States Bureau of Engraving & Printing.

Berlin Tunnel The Berlin Tunnel involved an attempt by American and British intelligence to adjust to the late 1940s Soviet shift from wireless transmissions to landlines by tapping Soviet and East German communication cables via a tunnel dug below the communist sector of the German city.

Binary weapon A chemical weapon in which two harmless agents are stored in separate containers and only mix to form toxic substance on contact with the target.

BINOCULAR NSA signals intelligence product.

BioAPI Biometric Application Programming Interface.

Biocontainment laboratories A laboratory that has been designed to lessen or completely prevent the escape of microorganisms.

Biodetectors Analytical devices that combine the precision and selectivity of biological systems with the processing power of microelectronics.

Bioflips Specialized microprocessors that can be implanted in the body and that are capable of configuring and calibrating themselves internally via biological feedback (e.g., a response to a set of biological conditions or parameters).

Biological warfare As defined by The United Nations, the use of any living organism (e.g. bacterium, virus) or an infective component (e.g., toxin), to cause disease or death in humans, animals, or plants. In contrast to bioterrorism, biological warfare is defined as the "state-sanctioned" use of biological weapons on an opposing military force or civilian population. Biological weapons include pathogenic viruses, bacteria, and biological toxins.

Biological weaponization Putting a pathogen in a form or suspension to make it an effective military weapon.

BioMagnetICs Bio-Magnetics Interfacing Concepts.

Biometrics An automated technique measuring physical characteristics (such as fingerprints, hand geometry, iris, retina, or facial features) of an individual for the purpose of identification or authentication of that individual.

BIOS Biological Input/Output Systems program.

BioShield project A joint effort between the Department of Homeland Security and the Department of Health and Human Services, Project BioShield is tasked to improve treatment of diseases caused by biological, chemical and radiological weapons.

Bioterrorism The use of a biological weapon against a civilian or military population by a government, organization, or individual. As with any form of terrorism, its purposes include the undermining of morale, creating chaos, or achieving political goals. Biological weapons use microorganisms and toxins to produce disease and death in humans, livestock, and crops.

BIS (Bezpecnostni Informacni Sluzba) Czech Security Information Service.

Bitstream embedding The insertion of message data in digital documents or data streams that contain enough redundancy that some of their information can be altered without obvious effect. For instance, one might conceal a message bitstream inside a digital audio file by replacing the least-significant bit of every waveform sample (or every *n*th waveform sample).

Black chamber The term "black chamber" has come to represent any code-breaking organization, but was originally applied to groups of code-breakers associated with a nation's Post Office that intercepted, read, copied and decoded diplomatic mail.

Black ops Shorthand for "black operations," covert or clandestine activities that cannot be linked to the organization that undertakes them.

Black September aka/see: Abu Nidal Organization (ANO).

Black Tom explosion The peak act of German sabotage on American soil during the First World War. On July 29, 1916, German agents set fire to a complex of warehouses and ships in the New York harbor that held munitions, fuel, and explosives bound to aid the Allies in their fight.

BLACKER NSA end-to-end encryption system.

Blackmail The threat to expose an individual's illegal or immoral acts if the individual does not comply with specific demands.

Bletchley Park The headquarters of the British Military Intelligence Government Code and Cipher School during World War II.

Block cipher A cipher that transforms fixed-length blocks of plaintext into ciphertext and vice-versa.

Bludgeon A general term for any weapon that consists of a short stick with one end weighted. Examples are the blackjack or cosh.

BMDO The Ballistic Missile Defense Organization (BMDO), the successor to the Strategic Defense Initiative Organization in the United States Department of Defense, develops systems to detect, track, and destroy ballistic missiles.

BND German Bundesnachrichtendienst.

Bombe A mechanical device used for the rapid decryption and transcription of complex ciphers. Developed during World War II, the multiple bombes employed by British and United States military intelligence code breakers aided the allied war effort by providing access to German and Japanese military secrets.

Bomb-grade nuclear materials Bomb-grade uranium or plutonium is defined as any alloy of uranium or plutonium that is pure enough to be used in bombs.

Bona fides An individual's verified qualifications, credentials, or background history.

Boost phase That part of a ballistic weapon's flight path during which it is being accelerated (boosted) by its rockets.

BOSS Bio-Optic Synthetic Systems.

Botulinum toxin Botulinum toxin is among the most poisonous substances known. The toxin, which can be ingested or inhaled, and which disrupts transmission of nerve impulses to muscles, is naturally produced by the bacterium *Clostridium botulinum*. Certain strains of *C. baratii* and *C. butyricum* can also be capable of producing the toxin.

Brainwashing An attempt to tear down an individual's former beliefs and replace them with new ones through an intense psychological and sometimes physical process.

Brain-wave scanner In conjunction with MRI, brain-wave scanners research is devoted to developing electronic equipment able to predict whether an individual is lying or concealing the truth in statements.

Brute force A method of decryption in which a cryptanalyst, lacking a key, solves a cipher by testing all possible keys. This tends to be impractical for most ciphers without the

use of a computer, and for the most sophisticated modern ciphers, brute force is all but impossible.

BTS Directorate of Border and Transportation Security (BTS), Department of Homeland Security.

Bucket dropper A spy satellite that takes pictures on film and returns the film to Earth for analysis.

Bug Intelligence and security slang for an electronic device consisting of a microphone and a radio transmitter.

C3 A U.S. Department of Defense abbreviation for command, control, and communications.

C4 A U.S. Department of Defense abbreviation for command, control, communications, and computers.

CAM Chemical Agent Monitoring device.

Camouflage Derived from the French *camoufleur* ("to disguise"), the term "camouflage" entered the English language during World War I, when the development of military aircraft exposed troop positions to enemy reconnaissance planes. Camouflage seeks to obscure or "hide in place."

Candestine information Information obtained without either the knowledge or consent (e.g. classified or secret information obtained from foreign governments).

CAP Continuous assisted performance.

CAPPS Computer Assisted Passenger Pre-Screening System.

CAPS Computer Assisted Passenger Screening System.

Carrier battle group A force of a half-dozen or more ships, with an aircraft carrier as its centerpiece, that includes destroyers, frigates, cruisers, submarines, and supply vessels.

Carrier current Transmission of low-frequency radio signals on power or telephone lines.

Carrier to Noise ratio (C/N) A ratio used to measure and denote signal quality. The greater the ratio the better the signal.

Carriers Charge-carrying particles in semiconductors, electrons, and holes.

Case An entire intelligence operation.

Case officer An intelligence officer whose job it is to supervise agents working on a case.

Catalog number A unique number issued by NASA that identifies a satellite.

CATIS/IESS Computer Aided Tactical Information System/ Imagery Exploitation Support System.

CB Chemical and biological.

C-band Multiple channels with horizontal and vertical uplinks and downlinks. Downlinks: 3.720–4.180 GHz; Uplinks: 5.945–6.405 GHz.

CBEFF Common Biometric Exchange File Format.

CBIAC The Chemical and Biological Defense Information Analysis Center (CBIAC) is a civilian-operated institution that contracts with the United States Department of Defense (DOD) to provide information on chemical and biological warfare technology.

CBIRF The Chemical and Biological Incident Response Force (CBIRF) is a unit of the United States Marines devoted to countering chemical or biological threats at home and abroad.

CBNP Chemical and Biological National Security Program (CBNP), United States Department of Energy (DOE).

CCCP Central Committee, Communist Party, Soviet Union (USSR).

CCDB Common Cryptologic Database.

CCOP Cryptologic Carry-On Program.

CCSE Canadian Communications Security Establishment.

CCSEW Canadian Communications Security Establishment.

CCTV Closed-circuit television (CCTV) involves the use of video cameras to produce images for display on a limited number of screens connected directly to a non-broadcast transmission system (e.g., a network of cables).

CDC Centers for Disease Control and Prevention. The center, which is headquartered in Atlanta, Georgia, is one of the predominant public health institutions in the United States and in the world. The CDC serves United States national security by monitoring the incidence of infectious disease in the United States (and around the world), and through the development and implementation of disease control procedures.

CDIS Counter Drug Intelligence System.

CE Counter-espionage.

Cell Most fundamental or basic unit of a network (e.g. terrorist network).

Cells Biology: The smallest living units of the body which together form tissues.

CERN Located along the French-Swiss border near the Swiss capital Geneva, CERN is the world's largest particle-physics laboratory. (The acronym stands for Conseil Européenne pour la Recherche Nucléaire, French for CERN's original name, the European Council for Nuclear Research; since October 56, 1954, despite retention of the old acronym, CERN's name has actually been *Organization* Européenne pour la Recherche Nucléaire.)

CES Collection Evaluation System.

CESG United Kingdom Communications-Electronics Security Group.

CFF Cambodian Freedom Fighters.

CGNRC Coast Guard National Response Center.

Chemical warfare The aggressive use of bulk chemicals that cause death or grave injury. These chemicals are different from the lethal chemical compounds that are part of infectious bacteria or viruses.

Chernobyl On April 26, 1986, a nuclear reactor in the town of Chernobyl (in the Ukraine, then a member state of the Soviet Union) exploded, collapsing the building in which it was located and releasing a radioactive plume that deposited material over much of Europe and Scandinavia.

Chief of mission The leading representative of the U.S. president in a host nation—usually an ambassador.

China syndrome A hypothetical nuclear power plant accident in which the molten uranium of the ruined core will coalesce into a single superheated mass and melt its way down to the groundwater below the plant, causing a violent steam explosion and dispersing even larger quantities of radioactive material.

Chlorine gas Lung irritant generally mixed with phosgene.

Chromatography Techniques for separating molecules or compounds based on differential absorption and elution.

CIA United States Central Intelligence Agency.

CIAO Critical Infrastructure Assurance Office.

CIAP Command Intelligence Architecture Planning Program.

CIB Controlled Image Base.

CIBS-M Common Integrated Broadcast Service Modules.

CIC United States Counterintelligence Center.

CIG Central Intelligence Group.

CIGSS Common Imagery Ground/Surface System.

CI/HUMINT Counterintelligence/Human Intelligence.

CIPA The Classified Information Act, passed by Congress in 1980. CIPA presents guidelines for the use of classified information by both government and defendant in a legal case.

Cipher A cipher uses a system of fixed rules (an algorithm) to transform a legible message (plaintext) into an apparently random string of characters (ciphertext).

Cipher disk A handheld coding device for generating a limited number of substitution ciphers, that is, ciphers in which each letter of the regular alphabet is enciphered as a single character from a cipher alphabet.

Cipher key A sequence of symbols that a user of a given cipher system must possess in order to use the system. Without a key, a user cannot encipher messages (turn them from plaintext to ciphertext) or decipher messages (turn them from ciphertext to plaintext).

Cipher machine A mechanical device that assists in the production of ciphertext from plaintext and vice versa. In this broad sense, any mechanical aid from a cipher wheel to a supercomputer can qualify as a cipher machine; however, the term is usually reserved for devices that are fairly complex and that operate on mechanical or electromechanical rather than on electronic principles.

Cipher pad A printed list of cipher keys, each intended to be used for the encipherment and decipherment of a single message. Cipher pads (also termed one-time pads) are closely related to one-time tapes and stream ciphers.

Cipher text Series of symbols produced by a cipher to convey a message; intended to be unreadable by unauthorized persons.

Ciphony The scrambling through technology of the spoken word.

CIRA Continuity Irish Republican Army.

CITA DOE Counterintelligence Training Academy.

Clam dead drop A tiny metal chamber used for concealing materials to be transferred at a dead drop. Attached to the chamber is a magnet, such that it can be attached to an inconspicuous place on a car or any other large object with metallic parts.

Clandestine operation A covert or secret operation.

Clarke belt A geostationary orbit named for author Arthur C. Clarke, an early proponent of the orbit.

CLASS Consular Lookout and Support System.

Classified information Materials or data belonging to, controlled by, and/or produced by the federal government, pertaining to intelligence sources or methods of collecting information; cryptology or codes; and the vulnerabilities, capabilities, or planning of systems, installations, or projects that relate to national security.

Clipper chip Devices that permit secure encrypted voice communications, but also allow United States law enforcement and intelligence agencies to monitor those communications by obtaining the algorithm keys to decrypt the transmissions.

CNC Crime and Narcotics Center.

Cobbler A forger of false documents, including identification papers (e.g. passports, visas, birth certificates, etc.).

Code A system for concealing a message by replacing words or phrases with symbols. It is distinguished from a cipher in that the latter replaces each letter of a plain-text message, whereas a code replaces entire words or phrases in such a way that there is no one-to-one correspondence.

Code name A word or phrase used to refer secretly to a specific person, group, project, or plan of action. Individual spies and large-scale military operations are often referred to by code names to protect their identity.

Code word A word or phrase that is used to convey a predefined message that differs from its own literal meaning.

Codes and ciphers Forms of cryptography, a term from the Greek *kryptos*, hidden, and *graphia*, writing. Both transform legible messages into series of symbols that are intelligible only to specific recipients. Codes do so by substituting arbitrary symbols for meanings listed in a codebook; ciphers do so by performing rule-directed operations directly on original message text.

Cognitive computers Computing systems designed to learn and adapt their programming.

Coin knife A small, blunt knife—more effective for the purposes of escape than for inflicting bodily harm—attached to the back of a large coin by a hinge.

COINS Community On-line Intelligence System.

COINTELPRO (*Co*nter *Intel*ligence *Pro*gram). A set of programs commenced by the United States Federal Bureau of Investigation (FBI) in 1956 and officially terminated in 1971. COINTELPRO included programs variously named Espionage COINTELPRO; New Left COINTELPRO; Disruption of White Hate Groups (targeting the Ku Klux Klan); Communist Party, USA COINTELPRO; Black Extremists COINTELPRO; and the Socialist Workers Party.

Cold war An ideological, political, economic, and military conflict primarily between the United States, United Kingdom and Western allies against the Union of Soviet Socialist Republics (U.S.S.R.) and Soviet dominated Eastern bloc

nations that began in the aftermath of World War II and ended in 1989. From the outset, the cold war was inextricably linked with the development of the atomic bomb and its use as a military deterrent.

Collection Obtaining, assembling and organizing information for further intelligence use.

Colossus I The world's first programmable computer. Colossus I was created during World War II by the British to speed up the decryption of German messages encoded by the Lorenz Schlüsselzusatz (SZ) 40 and 42 machines.

COMINT Communications intelligence, or intelligence gained through the interception of foreign communications, excluding open radio and television broadcasts. COMINT is, along with ELINT or electronic intelligence, one of two subsets of signals intelligence (SIGINT).

Company, The The nickname for the CIA (United States Central Intelligence Agency).

Compartment A group of individuals with a "need to know," and thus with specialized security access, for a specific topic.

Comprehensive Test Ban Treaty An international agreement designed to end the testing of nuclear explosives. As of March 2003, the United States is one of the 166 states that have signed the treaty, but the CTBT will only "enter into force" (i.e., take on the force of law for all ratifying states) when forty-four "nuclear-capable" countries specifically listed in the treaty have all ratified the treaty.

Compute modeling Modeling, in the technical use of the term, refers to the translation of objects or phenomena from the real world into mathematical equations.

Computer Fraud and Abuse Act of 1986 The Computer Fraud and Abuse act served to define criminal fraud and abuse for computer crimes on the federal level.

Computer keystroke recorder A program that runs in the background as a computer operates, sequentially recording all keystrokes. Also called a keystroke logger, key logger, or keylogger.

Computer Security Act of 1987 The first major U.S. government effort to legislate protection and defense for unclassified information in government-related computer systems.

Computer virus A program or segment of executable computer code that is designed to reproduce itself in computer memory and, sometimes, to damage data.

Confidential The lowest U.S. general security classification. A term referring both to information whose disclosure to unauthorized personnel could reasonably be expected to cause damage to national security, and to the security clearance necessary to access such information.

Contact An agent who serves as a liaison.

Continuous assisted performance (CAP) Programs that are designed to allow an increase in operation tempo by allowing soldiers to operate without sleep, or limited amounts of sleep.

Control The supervising officer or agent.

CONUS Continental United States.

Co-option The taking over and controlling of a spy from one intelligence service to another.

Copyright laws Laws that protect the rights of authors and artists by assuring them the exclusive legal right to reproduce, distribute, perform, display, or license work, as well as derivatives of the work.

Counterintelligence The use of intelligence resources to identify, circumvent, and neutralize the intelligence activities of a foreign power.

Countermeasures Techniques designed to defeat a defensive system.

Courier An agent who retrieves and delivers messages.

Cousins A name for the CIA used by British intelligence.

Cover A business/trade front which conceals espionage operations.

Coverage In electronics use: An area where a signal can be received.

Covert operations Activities that are carried out by an intelligence or security agency, usually in a foreign country, in such a way that it is difficult to connect that agency with its action.

CPNB Chemical and Biological National Security Program.

CPSC Consumer Product Safety Commission.

Crib A section of an encoded or enciphered message that can easily be rendered into plain text, thus providing a tool whereby a skilled cryptanalyst can crack the entire code or message.

Critical infrastructure A general term for physical and computer-based systems essential to the functions of the government and economy. Among these are telecommunications, energy, banking and finance, transportation, water systems, and emergency services.

CRS Comprehensive radiation sensors.

Cruise phase Portion of a ballistic missile's flight during which the payload has separated from the booster but has not yet begun to descend toward its target.

Cryptography The use of messages concealed by codes or ciphers.

Cryptology The study of both cryptography and cryptanalysis.

Cryptonym Cryptonyms, or code names, are words, symbols, or numbers used in place of the actual name of a person, item, or planned event.

Crytanalysis The breaking of coded messages without prior possession of the key.

CSE United States Center for Security Evaluation.

CSI The Center for the Study of Intelligence (CSI) of the United States Central Intelligence Agency (CIA) is a reference and resource center for scholars and others studying the history and practice of intelligence disciplines.

CSIC Canadian Security and Intelligence Community.

CSIL Commercial Satellite Imagery Library.

CSIS Canadian Security Intelligence Service.

CSIS Center for Strategic and International Studies.

CT CT scanners.

CT product Mathematical product of concentration (mg/m^3) multiplied by time of exposure in minutes.

CTBT Comprehensive Test Ban Treaty.

CURV Cable-Controlled Undersea Recovery Vehicle.

Customs Service United States Customs Service (previously part of the Department of Treasury). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).

Cut and cover A type of underground construction in which a structure is built within an excavated area and then covered with soil or rock.

Cutout An agent who serves as a liaison.

CX Phosgene oxime or dichloroform oxime.

Cyber security Measures taken to protect computers and computer networks from accidental or malicious harm.

Cyberattack An assault on the security of a computer system, usually by a hacker or other cybercriminal.

Cybercrime Criminal activity involving the use of a computer.

Cyclosarin nerve agent GF; Cyclohexyl methylphosphonofluoridate.

D notice (defense notice). An alert given by British intelligence services or the armed forces to the media, alerting them of sensitive content that could damage national security or defense if reported in part or in whole.

DACS Deportable Alien Control System.

Dagger A short knife, made for the purpose of stabbing rather than cutting.

DAIRS DIA Advanced Imagery Reproduction System.

DARPA Defense Advanced Research Projects Agency.

DARTS Design and Analysis of Reference Threat Signature.

DASC Deportable Alien Control System.

Data mining Statistical analysis techniques used to search through large amounts of data to discover trends or patterns.

DAWS Defense Automated Warning System.

DBS Direct Broadcast Satellite.

dBW The ratio of the power to one Watt in decibels.

DC power Direct current power.

DCI Director of the Central Intelligence Agency.

DCIIS Defense Counterintelligence Integrated Information System.

DCP Data Collection Platform.

DCS Defense Communications System.

DDN Defense Data Network.

DDS Defense Dissemination System.

DE DDS Dissemination Element.

DEA Drug Enforcement Administration.

Dead drop A prearranged spot at which one party passes information to another without actually meeting; or, the act of making such a transfer, as in "making a dead drop." Often a dead drop also involves the transfer of money, as when a double agent leaves information for a handler, and the handler returns the favor with a cash payment.

Dead-drop spike A device, resembling a large, fat pencil, used for making dead drops. The blunt end has a cap that can unscrew, so that materials can be inserted into the air- and watertight chamber, while the pointed end makes it easy to hide the spike in the ground.

Dead-letter box A covert location where messages or other items are deposited for retrieval by other intelligence operatives. Also called a dead drop, they are most often used as a means of transferring documents and messages, but can also be used to funnel equipment and money to agents in the field.

Debriefing The process of interrogation, often planned and voluntary, designed to elicit information after a specific mission, event, or term of service.

Declassification The removal of restrictions on access to information. In some cases, declassification of a document is automatic after a certain period of time; in others, security considerations dictate a continuation of the classified status.

Decontamination The efforts to safeguard property and people that have been exposed to chemical, nuclear, or biological agents.

Decryption The reverse of encryption, the process by which ordinary data, or plain text, is converted into a cipher. To decipher a message requires a key, an algorithm that provides the method by which the message was encrypted.

Deep cover An agent who operates under many layers of legends or false backgrounds.

Defector A spy who voluntarily changes sides or leaves service to aid an "enemy" country or organization.

Defector-in-place Any agent who defects to the opposing side but who remains in his prior position with the intent to act as a double agent.

DELTA force Elite counter-terrorism group of the U.S. Army's 1st Special Forces Operational Detachment-Delta.

DES Digital Encryption Standard. In the late 1970s, the U.S. government defined a cipher algorithm for standard use by all government departments, available also to the public. This early algorithm, the Digital Encryption Standard, is today in the process of being replaced by a new algorithm, the Advanced Encryption Standard.

Descent (or terminal) phase The final part of a ballistic weapon's flight path, during which the warhead falls through the atmosphere toward its target.

DEST Domestic Emergency Support Team.

Detonator A device that activates an explosion by subjecting a charge of explosive to a high-pressure shock wave.

DHKP Revolutionary People's Liberation Party/Front (DHKP/C).

DI Domestic Intelligence.

DIA Defense Intelligence Agency.

Dial tone decoder Telephone conversations are sometimes surreptitiously taped using microphones or other bugging devices. These devices run the risk of being detected. In some intelligence-gathering tapings, however, the contact telephone number may yield information that is as valuable as the actual conversation. If the content of a conversation is not essential, the contact telephone number can be obtained with a device called a dial tone recorder.

Dictionary In cyber intelligence: A computer programmed to scan intelligence data for specific terms and keywords.

DIEPS Digital Imagery Exploitation and Production System.

Digital stenanography The hiding of message data in a digital medium.

Digital watermarking Information indicating ownership or embedded in a digital file.

Diplomatic cover Any agent secretly working for the diplomatic corps of a foreign country.

Direction finder An electronic device—typically a radio of some kind—used to locate a source of electronic emissions such as a ship or aircraft.

Dirty bomb A conventional bomb usually packed with low-level radioactive debris that can be spread over a wide area when the explosive detonates.

Dirty tricks Clandestine activities carried out by a covert-action group to discredit, destabilize, or eliminate an opposing regime, one of its agencies or departments, or an individual. A type of covert operation, dirty tricks include everything from the spreading of false rumors to sabotage, overthrow, and assassination.

Disinformation Secret information altered or provided in such a way as to make that information appear to be genuine.

DISN Defense Information Systems Network.

DITDS Defense Intelligence Threat Data System.

DL/ID Driver's license and identification.

DMFE Defense Automated Warning System Message Front End.

DMS Defense Message System.

DNA Deoxyribonucleic acid. The molecular composition of genetic material that is, in part, made up of nitrogenous bases that form a genetic code.

DNA fingerprinting The term applied to a range of techniques that are used to show similarities and dissimilarities between the DNA present in different individuals.

DNA profile Evaluation of an individual's DNA to establish a unique pattern of markers that can be used for identification purposes.

DoD United States Department of Defense.

DODIIMS DoD Intelligence Management System.

DOE United States Department of Energy.

Domestic intelligence Efforts by a government to obtain information about activities that pose an actual or putative threat to internal security.

Doo transmitter A radio transmission device camouflaged as a pile of animal droppings or, in its most common form, a large single fecal dropping from an animal indigenous to the area of intended use.

Doppler radar Radar that detects the frequency shifts in echoes from moving reflectors, and so can determine speed as well as range of a target.

Double agent Someone who seems to serve one intelligence agency, but actually works on behalf of another.

Downlink A satellite to Earth connection or electronic signal path.

DPO Domestic Preparedness Office.

Drop Intelligence parlance for the location at which an agent passes information to another, or the act of passing that information—as in "making a drop."

DS United States Bureau of Diplomatic Security.

DS&T CIA Directorate of Science and Technology.

DSB Defense Science Board.

DSNET Defense Secure Network.

DSS Defense Security Service.

DTIC Defense Technical Information Center.

Dual use technology Tools or techniques, developed originally for military or related purposes, which are commercially viable enough to support adaptation and production for industrial or consumer uses.

Dynamic address A temporary Internet protocol (IP) address, assigned to a computer only during the time it is connected to the Internet.

EA Electronic Attack.

E-beam An irradiation method that can be used to decontaminate mail.

Ebola virus The species of Ebola virus are among a number of viruses that cause a disease, hemorrhagic fever, that is typified by copious internal bleeding and bleeding from various orifices of the body, including the eyes. The disease can result in death in over 90 percent of cases.

E-bomb An e-bomb, or electronic bomb, is a non-explosive artillery shell or missile that sends out an electromagnetic pulse (EMP) of enormous power, capable of permanently disabling mechanical and electronic systems.

ECCM Electronic Counter Counter Measures.

Echelon The name for a global surveillance network consisting of ground stations, satellites, and other listening posts, which collectively intercept and analyze worldwide electronic communications.

ECM Electronic Counter Measures.

Economic espionage Spying conducted for the benefit of a commercial or industrial enterprise, typically to gain information not available through open channels. Sometimes known as industrial espionage.

Edge weapons Knives and other devices with a sharp edge that can be used for murder or self-defense.

EEG Electroencephalogram.

EES Escrowed Encryption Standard program.

EIRP Effective Isotropic Radiated Power (a measurement of signal strength).

EIS Enhanced Imagery System.

EKMS Electronic Key Management System [NSA COMSEC].

ELA Revolutionary People's Struggle (ELA).

Electromagnetic pulse (EMP) Any nuclear explosion 25 miles (40 km) or higher above the ground produces a high-altitude electromagnetic pulse (HEMP), a short-lived, overlapping series of intense radio waves that blanket a large swath of ground. These radio waves can induce electrical currents in metallic objects and so cause damage to electrical and electronic equipment, including electrical power grids, telephone networks, radios, and computers.

Electromagnetic spectrum The complete range of electromagnetic waves on a continuous distribution from a very low range of frequencies and energy levels, with a correspondingly long wavelength, to a very high range of frequencies and energy levels, with a correspondingly short wavelength. Radio waves, visible light, and x rays are examples of electromagnetic waves at different frequencies. Every part of the electromagnetic spectrum is exploited for some form of military, security, or espionage activity; the entire spectrum is also key to science and industry.

Electronic countermeasures (ECM) An ECM, also known as an electronic attack, is a component of electronic warfare (EW), the use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. Its counterpart is electronic protection or electronic counter-countermeasures (ECCM)—efforts or equipment directed toward the protection of persons or material from the effects of electronic warfare.

Electronic warfare (EW) The use or control of electromagnetic energy either in defense, or for the purposes of a military attack on an enemy. There are three components of electronic warfare: electronic countermeasures or electronic attack, electronic counter-countermeasures or electronic protection, and electronic warfare support.

Electro-optical intelligence The acquisition of data from the portion of the electromagnetic spectrum of wavelengths that contains ultraviolet radiation, visible light, and infrared radiation.

ELINT Electronics intelligence, or intelligence derived from the interception of non-communication electromagnetic signals, most notably radar. Subsets of ELINT include FISINT, or foreign instrumentation signals intelligence, and TELINT, or telemetry intelligence. ELINT is in turn a subset of signals intelligence (SIGINT).

ELISA Enzyme-linked immunoadsorbent assay.

ELN National Liberation Army (ELN)-Colombia.

EM Electromagnetic.

EML Environmental Measurements Laboratory.

EMP Electromagnetic pulse—an energy surge from a mechanical, electrical, chemical, or nuclear system, which can be used as a weapon.

Encryption The conversion of a message from plain text into cipher or code.

Encryption of data Data is any useful information and encryption is any form of coding, ciphering, or secret writing. Encryption of data, therefore, includes any and all attempts to conceal, scramble, encode, or encipher any information.

Energy directed weapons Weapons that use energy to disable or destroy equipment or people are referred to as energy directed weapons. Examples include lasers, high-power microwave weapons, and charged particle beam weapons.

Energy harvesting The gathering of energy from ambient sources, including sunlight, wind, wave action, water currents, geothermal components such as volcanoes, chemical and thermal gradients, barometric fluctuations, electromagnetic radiation, and human and other biological systems.

ENIAC American Electronic Numerical Integrator and Computer.

Enigma A ciphering (code communication) system used by the German military from 1926 until the end of World War II, and by several other nations for some years after. Enigma was the first mechanized message-encryption system to see wide use.

Enrollment The initial collection of the biometric data for setting up templates.

Environmental security (DEM) Aspects of national security that are driven by or that address environmental issues, either domestically or globally.

Enzyme A type of protein that affects the rate of chemical reactions in the body.

EO United States presidential executive orders.

EOL As a technical abbreviation, most commonly used to denote "End of Life" the point at which a system becomes inoperational.

EPA Environmental Protection Agency.

EPCRA Emergency Planning and Community Right-to-Know Act, legislation passed by Congress in 1986 to help communities respond to chemical hazards.

EPDS Electronic Processing & Dissemination System.

Epitaxy The growth of crystalline layers of semiconducting materials in a layered structure.

EPR Directorate of Emergency Preparedness and Response, Department of Homeland Security.

Espionage The use of spies, or the practice of spying, for the purpose of obtaining information about the plans, activities, capabilities, or resources of a competitor or enemy. It is closely related to intelligence, but is often distinguished from it by virtue of the clandestine, aggressive, and dangerous nature of activities.

ETA Basque Fatherland and Liberty (ETA).

ETEP Emanated transient electromagnetic pulses.

Etiological Involving disease and the causes thereof.

EU European Union.

EURATOM European Atomic Energy Community.

EW Electronic warfare and techniques that utilize and exploit properties of the electromagnetic spectrum.

Executive order A guideline issued by the President of the United States, directed toward a particular issue, and possessing the status of a de facto law. Unlike presidential directives, executive orders are unclassified.

Executive Order 12863 Regarding: President's Foreign Intelligence Advisory Board.

Executive Order 12958 Regarding: Classified National Security Information.

Executive Order 12968 Regarding: Access to Classified Information.

Executive Order 12977 Regarding: Interagency Security Committee.

Executive Order 13224 Regarding: Freezing of terrorist organization assets.

Exhaustion Searching for a key or other secret quantity in code breaking by systematically checking all possibilities.

Exposure dose The quantity of a chemical that an organism receives from the environment through inhalation, ingestion, and/or contact with the skin.

Extradite To surrender an alleged criminal to another U.S. state or nation that has jurisdiction.

FAA United States Federal Aviation Administration.

Facility security The protection, and the measures taken toward the protection of a building or other physical location.

FAISS FORSCOM Automated Intelligence Support System.

FAM Federal air marshal.

FARC Revolutionary Armed Forces of Colombia (FARC).

Farm, The The nickname for the training school for CIA recruits in Virginia.

Fatwa A legal opinion or ruling issued by an Islamic scholar.

FBI United States Federal Bureau of Investigation.

FBIS CIA, Foreign Broadcast Information Service.

FCA Future Communications Architecture.

FCC Federal Communications Commission.

FDA United States Food and Drug Administration.

FDMA Frequency Division Multiple Access.

FDS Fixed Distributed System.

FEMA Federal Emergency Management Agency.

FEST United States Foreign Emergency Support Team.

FIA Future Imagery Architecture.

FIC Fleet Intelligence Center, which provided operational intelligence for the U.S. Navy from the 1960s until absorption of the FICs into the National Military Joint Intelligence Center (NMJIC) in 1991.

FINCEN Financial Crimes Enforcement.

Fingerprints The patterns on the inside and the tips of fingers. The ridges of skin, also known as friction ridges, together with the valleys between them form unique patterns on the fingers. Fingerprint analysis is a biometric technique comparing scanned image of prints with a database of fingerprints.

Firewall A system to prevent unauthorized access of computer hardware or software to or from a private network.

FISA The Foreign Intelligence Surveillance Act, which was passed by the United States Congress in 1978.

FISH German *Geheimschreiber* cipher machine.

FISINT Foreign instrumentation signals intelligence. Examples of FISINT include signals sent by foreign entities when testing and deploying aerospace, surface, and sub-surface systems. FISINT is a subset of ELINT, or electronic intelligence.

Fission A process in which the nucleus of an atom splits, usually into two daughter nuclei, with the transformation of tremendous levels of nuclear energy into heat and light.

FISTA Flying Infrared Signature Technology Aircraft.

Flame analysis A form of atomic emission analysis. The colors produced by the flame test are compared to known standards, and then the presence of certain elements in the sample can be confirmed. The color of the flame and its spectrum (component colors) is unique for each element.

FLETC Federal Law Enforcement Training Center (previously part of the Department of Treasury). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).

Flight Data Recorders Hardened mechanical devices, designed to survive a crash, that record measurements of an aircraft's performance, navigation and flight configuration.

Foggy Bottom Nickname for headquarters of the United States Department of State.

FOIA Freedom of Information Act. Sometimes known as the Freedom of Information-Privacy Acts, a term referring to 1967 (FOIA) and 1974 (Privacy Act) statutes and their amendments, which greatly restrict government agencies' authority to collect information on individuals, and to withhold that information.

Footprint A geographically related map of signal strengths.

Force projection The ability to project or move an aggregation of military personnel from the continental United States (or another theatre) in response to military requirements.

Foreign Broadcast Information Service (FBIS) The pre-eminent collector of open source information for the United States government; it collects, translates, and disseminates foreign open source material for U.S. government use. It started as the Foreign Broadcast Monitoring Service (FBMS).

Foreign Intelligence Surveillance Act Public Law 95–511, Foreign Intelligence Surveillance Act (FISA).

Forensic geology The use of geologic principles and techniques to establish facts or provide evidence used in a court of law. The gathering and interpretation of geologic data for intelligence, espionage, and national security purposes can fall under the second definition of forensic geology.

Forensic science A multidisciplinary subject used for examining crime scenes and gathering evidence to be used in prosecution of offenders in a court of law. Forensic science

techniques are also used to examine compliance with international agreements regarding weapons of mass destruction.

FORMMS Foreign Materiel Management System.

FORTEZZA NSA Crypto component of MISSI [formerly Tessera].

FPS Federal Protective Service (previously part of the General Services Administration). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).

FRVT Face Recognition Vendor Test.

FSB The Federal Security Service (a Russian intelligence organization formerly known as the FSK).

FSK The Federal Counterintelligence Service was a Russian intelligence organization that was later reorganized and renamed the FSB.

Fuselage The central portion of an aircraft, which usually holds passengers or cargo.

Fusion The process by which two light atomic nuclei combine to form one heavier atomic nucleus. As an example, a proton (the nucleus of a hydrogen atom) and a neutron will, under the proper circumstances, combine to form a deuteron (the nucleus of an atom of "heavy" hydrogen). In general, the mass of the heavier product nucleus is less than the total mass of the two lighter nuclei. Fusion is the initial driving process of nucelosynthesis.

G-2 The intelligence staff of a unit in the U.S. Army. It is contrasted with G-1 (personnel), G-3 (operations), and G-4 (supply). In the navy, these sections have their counterparts, each with an *N*-designation, while at the level of the Joint Staff, the sections use the prefix *J-*.

GA nerve agent Tabun, O-ethyl N,N-dimethylphosphoroamidocyanidate.

GAO United States General Accounting Office.

Gas chromatograph-mass spectrography (GC/MS) An instrument used to analyze the molecular and ionic composition of chemical compounds. GC/MS technology combines two widely used laboratory techniques: gas chromatography (GC), which separates and identifies compounds in complex mixtures, and mass spectrometry (MS), which determines the molecular weight and ionic components of individual compounds.

GB nerve agent Sarin; O-isopropyl methylphosphonofluoridate.

GBCS Ground-based common sensor.

GBS Global Broadcast Service.

GCHQ United Kingdom Government Communications Headquarters.

GD nerve agent Soman; O-pinacolyl methylphosphonofluoridate.

Genes Made up of DNA, a gene is found in the cell nucleus and carries in its sequence all the instructions for the development of an organism and all its traits.

Genetic information The total accumulation of known genetic data on all organisms. The term may also be applied to individuals or families, i.e., the total known genetic data for a given person or family group.

Genetic testing Any clinical or research assay that evaluates the genes, DNA sequence, or mutations in a specimen. This may include analysis of chromosomes, cells, enzymes, or molecular testing.

GENIE Genetic Imagery Exploitation.

Genome The entire DNA sequence containing an organism's genes.

GEO Geostationary earth orbit.

GEODSS Ground-based electro-optical deep space surveillance.

Geostationary orbit (GEO) A circular orbit at 35.780 km above Earth's equator that allows satellites to maintain a steady position relative to the terrain below as expressed in degrees meridian (i.e., east or west of the prime meridian).

Geosynchronous A satellite orbit that keeps the satellite at a fixed point relative to the rotating surface of the Earth.

Gestapo The *Geheime Staatspolizei*, or Gestapo, a German secret police force, was created in 1933 after Adolf Hitler became chancellor of Germany. The Gestapo was created to help solidify Nazi control by identifying and arresting anti-Nazi agents in Germany. The agency was restructured several times during its twelve-year history and was instrumental in perpetrating the Nazi deportation and destruction of European Jews during the Holocaust.

GF nerve agent Cyclosarin cyclohexyl methylphosphonofluoridate nerve agent.

GIA Armed Islamic Group (GIA).

GIS The common abbreviation for Geographic Information Systems, a powerful and widely used computer database and software program that allows scientists to link geographically referenced information related to any number of variables to a map of a geographical area.

Global Positioning System (GPS) A constellation of twenty-four navigational satellites orbiting Earth, launched and maintained by the U.S. military. GPS receivers can decode signals from the satellites to calculate location and exact time.

Globalization The integration of economies and markets worldwide.

Go pills Dexamphetamine pills used by soldiers to fight fatigue.

GPALS Global protection against limited strikes.

GPS Global positioning system.

GPU USSR State Political Directorate.

GRAPO First of October Antifascist Resistance Group.

Great Game In intelligence history, the "Great Game" described a complex rivalry—characterized by wars, assassinations, and espionage conspiracies—between Britain and Russia for control of Central Asia and the Near East.

GRIS Global Reconnaissance Information System.

GRU USSR Military Intelligence.

GSA General Services Administration.

GSD Graphical situation display.

GSM encryption GSM stands for either "group special mobile" or "general system for mobile communications," a protocol or standard for digital cellular communications. GSM encryption is the means by which phone conversations on networks using GSM are scrambled, such that they cannot be descrambled and intercepted by others.

GSPC Salafist Group for Call and Combat.

GSR Ground surveillance radars.

GSS Israeli General Security Service.

G/T Unit of measurement for an antenna derived from the gain and noise temperature. Generally, the higher the G/T ratio the stronger the antenna.

GTO Geostationary transfer orbit. Generally used to refer to the temporary orbit of a geostationary satellite destined for GEO orbit.

Guerilla warfare In the modern era, guerilla warfare refers to armed resistance by paramilitary or irregular groups toward an occupying force. Guerilla warfare also describes a set of tactics employed by smaller forces against larger, better equipped, and better supplied forces.

HAARP ELF/VLF radio detection of underground structures.

Habeas Corpus U.S. constitutional right to avoid unlawful detention or imprisonment. Taken from the Latin phrase "You have the body."

Hacker A person who gains illegal access to, and sometimes tampers with, computer systems and the information they contain.

Hacktivism The use of computer hacking in the service of political activism.

HAHO A high altitude-high opening parachute jump.

HALO A high altitude-low opening parachute jump.

HAMAS Islamic Resistance Movement (HAMAS).

HAMMER Hazardous materials management and emergency response.

HANAA Nucleic acid analyzer.

Handler A case officer who works on a one-on-one basis with an agent.

Hardening In a general sense, hardening is the process of securing a computer. More specifically, hardening is the removal or disabling of all components in a computer system that are not necessary to its principal function or functions.

Hemorrhagic fevers and diseases Hemorrhagic diseases are caused by infection with viruses or bacteria. As the name implies, a hallmark of a hemorrhagic disease is copious bleeding.

Hertz (Hz) Unit of frequency; 1 Hz equals one cycle per second.

HEU Highly-enriched uranium.

HF-band 1.8–30 MHz.

HHS Health and Human Services Department.

High-power microwave (HPM) weaponry High-power microwave weaponry sends out a short, extremely high-voltage burst of electromagnetic energy capable of disrupting computer systems for a fraction of a second.

HIMS Human information management system.

HPSC High Performance Scientific Computing Research System.

HSMN Homeland Security Monitoring Network.

HT A mixture of distilled mustard gas compound and Agent T.

HUAC U.S. House Un-American Activities Committee.

HUJI Harakat ul-Jihad-I-Islami.

HUJI-B Harakat ul-Jihad-I-Islami/Bangladesh.

HUM Harakat ul-Mujahidin (Movement of Holy Warriors).

HUMINT Human intelligence, the gathering of information through human contact. HUMINT is, along with signals intelligence and imagery intelligence (SIGINT and IMINT respectively), one of the three traditional means of intelligence-gathering.

Hydrophone An underwater microphone sensitive to acoustic disturbances.

Hypersonic aircraft A plane capable of flying at Mach 5, or five times the speed of sound. At sea-level atmospheric pressure, with air temperatures of 59°F (15°C), the speed of sound is about 760 miles per hour (1,225 k.p.h.).

IAA Islamic Army of Aden.

IAEA International Atomic Energy Agency.

IAFIS Integrated automated fingerprint identification system (FBI system).

IAIP Information Analysis and Infrastructure Protection, Department of Homeland Security.

IAS Intelligence Analysis System.

IBIS The Interagency Border Inspection System (IBIS) is a database of names and other identifying information used to deter and append suspects—including suspected terrorists—as they attempt to pass through international border crossing checkpoints.

IBS Integrated Broadcast Service.

IC4I Integration for Command, Control, Communications, Computers and Intelligence.

ICARIS Intelligence Communications and Requirements Information System.

ICBM Intercontinental ballistic missile.

IDC International Data Centre.

IDENT The Automated Biometric Identification System (IDENT) is a database system using automated fingerprint identification systems (AFIS) technology as part of programs supervised by the U.S. Department of Homeland Security that intend to thwart illegal entry into the United States by criminal aliens.

Identification In biometrics, a one-to-many comparison against the entire enrolled population.

Identity theft An identity thief typically obtains access to a victim's social security number, driver's license information, bank account numbers, credit card numbers, etc. with the intent to open accounts in the victim's name and make purchases or perform other transactions.

IDHS Intelligence data handling system.

IESA International Environmental Sample Archive.

IFF Identification friend or foe (IFF) systems are a means of identifying aircraft, ships, and vehicles using electronic means. Applied by both military and civilian entities, IFF—which in its civilian form is more properly known as the air traffic control radar beacon system, or ATCRBS—uses radar to identify aircraft, which are assigned unique identifier codes. There are various modes of operation for IFF, depending on the level of security desired.

IFSARE Interferometric synthetic aperture radar—elevation.

IG Al-Gama'a al-Islamiyya (Islamic Group, IG).

Image intensification Amplification of dim patterns of reflected light to make a visible image; used in night-vision scopes.

IMETS Integrated Meteorological System.

IMF International Monetary Fund.

IMINT Imagery intelligence, or intelligence derived from photography, infrared sensors, synthetic aperture radar, and by other forms of imaging technology. Once known as PHOTINT or photographic intelligence, IMINT is one of the four major branches of intelligence, along with HUMINT, MASINT, and SIGINT (human, measurement and signatures, and signals intelligence respectively).

IMS International Monitoring System.

IMU Islamic Movement of Uzbekistan.

Inclined orbit A satellite with a figure "8" like orbit that travels across Earth's equator.

Indications and warnings (IW) Intelligence that relates to time-sensitive information involving potential threats.

INF United States Bureau of Intelligence & Research.

Infectious diseases Diseases that are caused by micro-organisms such as bacteria and viruses, many of which are spread from person to person. An intermittent host, or vector, aids the spread of some infectious diseases.

Information security Information security, often compressed to "infosec," is the preservation of secrecy and integrity in the storage and transmission of information.

Information warfare A general term encompassing a variety of tools and techniques, including psychological warfare, jamming of broadcasts, computer hacking, and cyberwarfare.

Infrared detection devices Sensors that detect radiation in the infrared portion of the electromagnetic spectrum ($>10^{12}$ to 5×10^{14} Hz).

Infrared imaging Detection of infrared radiation emitted by objects in a scene followed by creation of a visible-light image.

INL International Narcotics and Law Enforcement Affairs, United States Bureau for.

INM Bureau of International Narcotics Matters.

INS As of March 1, 2003, the newly created United States Department of Homeland Security (DHS) absorbed the former Immigration and Naturalization Service (INS). All INS border patrol agents and investigators—along with agents from the U.S. Customs Service and Transportation Security Administration—were placed under the direction of the DHS Directorate of Border and Transportation Security (BTS). Responsibility for U.S. border security and the enforcement of immigration laws was transferred to BTS. Former INS immigration service functions are scheduled to be placed under the direction of the DHS Bureau of Citizenship and Immigration Services. Under the DHS reorganization plan, the INS formally ceases to exist on the date the last of its functions are transferred.

INSC International Nuclear Safety Center.

INSCOM U.S. Army Intelligence and Security Command.

INSPASS Immigration and Naturalization Service Passenger Accelerated Service System.

Integrated circuits Complex electronic circuits fabricated using multiple growth and lithography/pattern transfer stages to produce many miniature electronic elements on a monolithic device.

Intelligence Information concerning a foreign entity, usually (although not always) an adversary, as well as agencies concerned with collection of such information. It is intimately tied with the intelligence cycle, a process whereby raw information is acquired, converted into intelligence, and disseminated to the appropriate consumers.

Intelligence agent In general terms, an agent is one authorized to act in place of, or on behalf of, another. An intelligence agent, however, is not simply an agent of or for an intelligence agency. Whereas members of the agency are called intelligence officers, operatives, or special agents, an agent is someone hired or recruited from outside. There are numerous other variations in the informal taxonomy of agents, including secret or undercover agents, agents provocateur, agents-in-place, double agents, etc.

Intelligence Authorization Act The 1981 congressional act that established the process whereby the CIA notifies the leadership of the House and Senate Intelligence Committees of covert actions.

Intelligence officer A professional employed by an intelligence service. Members of the intelligence community make sharp distinctions between intelligence officers and intelligence agents, who are outsiders employed by the intelligence agency. Intelligence officers, on the other hand, are operatives of the agency itself, but their professional role—and the fact that many are military officers and/or intelligence specialists—gives them particular distinction.

Intercept Intelligence gathered through electronic eavesdropping.

Internet A vast worldwide conglomeration of linked computer networks. The most significant component of the Internet is the World Wide Web.

Internet dynamic and static addresses Every computer operating on the Internet has a unique IP, or Internet protocol, address. Because the Internet's original design did not take into account the vast size it would assume from the mid-1990s onward, as more and more people went online, the architecture did not account for an infinite number of IP

addresses. To conserve these, an Internet service provider (ISP) has a limited number of permanent IP addresses, and issues temporary IP addresses for customers to use while online.

Internet Spider A program designed to "crawl" over the World Wide Web, the portion of the Internet most familiar to general users, and retrieve locations of, and information from Web pages.

Internet surveillance The monitoring of Internet data traffic for information useful to government authorities.

Internet tracking and tracing Electronic passage through the Internet leaves a trail that can be traced. Tracing is a process that follows the Internet activity backwards, from the recipient to the user.

INTERPOL International Criminal Police Organization.

Interrogation A conversational process of information gathering. The intent of interrogation is to control an individual so that he or she will either willingly supply the requested information or, if someone is an unwilling participant in the process, to make the person submit to the demands for information. The latter can involve techniques of humiliation, intimidation, and fear. In more extreme cases, in some countries, physical pain is inflicted.

Intifada Literally, "shaking off," a term applied to the Palestinian uprising against Israel's occupation of the West Bank and Gaza.

IOL Inter-orbit link.

IOM Institute of Medicine.

IOSA Integrated Overhead SIGINT Architecture.

IPDS Imagery Processing & Dissemination System.

IPL Imagery Product Library.

IRA Irish Republican Army.

Irradiation Using radiation, primarily for sanitization purposes, such as in use for irradiating mail by the United States Postal Service.

IRS Internal Revenue Service.

ISAR Inverse Synthetic Aperture Radar.

ISFAR Interferometric Synthetic Aperture Radar.

ISMC Intel Link Systems Management Center.

ISMS Integrated Security Management System.

Isotope A form of a chemical element distinguished by the number of neutrons in its nucleus. E.g., ^{233}U and ^{235}U are two isotopes of uranium; both have 92 protons, but ^{233}U has 141 neutrons and ^{235}U has 143 neutrons.

IT Information technology, a term that encompasses computers and related materials, machines, and processes.

IUSS Integrated Undersea Surveillance System.

IW Indications and warnings. Intelligence that relates to time-sensitive information involving potential threats.

J-2 Joint intelligence, the office supporting the intelligence needs of a joint or unified command. For the Joint Chiefs of Staff, the Defense Intelligence Agency serves the J-2 function.

Jamming Blocking of electronic signals.

JDAM Joint Direct Attack Monition (JDAM) is a satellite-guided "smart" bomb capable of accurate and high precision strikes in any weather.

JDISS Joint Deployable Intelligence Support System.

JEM Jaish-e-Mohammed (Army of Mohammed).

JI Jemaah Islamiya.

JIC Joint intelligence center, or the intelligence center of a command headquarters. For the Joint Chiefs of Staff, the National Military Joint Intelligence Center serves this function.

Jihad In Islam: A holy struggle or war.

JIRONET Joint Intelligence Research Office Network.

JMIP The Joint Military Intelligence Program, an annual budget request for military intelligence presented by the Secretary of Defense to the President of the United States.

JN-25 Japanese Navy-25, the name given to the Japanese military operational code during World War II.

JRA Japanese Red Army.

JSTARS Joint Surveillance Target Attack Radar System.

JSTARS-CGS JSTARS Common Ground Station.

JSTARS-GSM JSTARS Ground Station Module.

JTT Joint Tactical Terminal.

JUI-F Jamiat Ulema-I-Islam Fazlur Rehman faction.

JWICS Joint Worldwide Intelligence Communications System.

Ka-band Generally between 18 to 31 GHz.

Key An algorithm that provides the method by which a message was encrypted.

Keyhole Since 1962, code name for US photoreconnaissance satellites.

KGB USSR *Komitet Gosudarstvennoi Bezopasnosti* (Committee of State Security). The USSR equivalent of the American CIA.

KH Cameras, KH series.

Kiloton A measure of energy used to quantify the size of large explosions, especially nuclear explosions. One kiloton is equivalent to the energy produced by the explosion of 1000 tons of TNT.

KMM Kumpulan Mujahidin Malaysia.

LANL Los Alamos National Laboratory.

L-band 1.530–2.700 GHz.

LBNL Lawrence Berkeley National Laboratory.

LC50 The chemical concentration required to kill 50 percent of test subjects.

LCL0 The minimal chemical concentration found to be lethal.

LD50 Lethal dose for 50 percent of those exposed to a toxic agent.

LDL0 The minimal dose strength found to be lethal.

L-Gel decontamination reagent A coating that was developed at Lawrence Livermore National Laboratory (LLNL) in Berkeley, California. The coating is effective at decontaminating areas exposed to both chemical and biological agents.

Legend A false background or biography.

LEO Low earth orbit.

LEPC Local Emergency Planning Committee.

Less lethal weapons Tools and techniques designed for riot control and other security functions with the intention of neutralizing hostile activity without killing or causing permanent bodily harm.

Lewisite blistering agent Chlorovinyldichloroarsine.

Light detection and ranging (LIDAR) An active remote sensing system that allows exceptionally accurate and rapid determination of terrain and structural features (e.g. height). LIDAR produces highly accurate three dimensional data measurements that can then be utilized by mapping, guidance, and navigation systems.

LLNL Lawrence Livermore National Laboratory.

LNA Low-noise amplifier.

LOCE Linked Operations/Intelligence Centers Europe.

Lock-picking An ability to open locks without the key specific for the lock.

Looking Glass The nickname for the Airborne Command Post, a mission operated continuously by U.S. Strategic Air Command (SAC) between 1961 and 1990. For almost three decades, SAC had an aircraft aloft 24 hours a day, seven days a week.

Lord Haw-Haw The nickname of Nazi propagandist and broadcaster, William Joyce. During World War II, Joyce broadcast a well-known English-language propaganda show from Berlin, often taunting Allied forces. Though never calling himself Lord Haw-Haw on air, he became infamous among Allied combat troops and British citizens.

LRA Lord's Resistance Army.

LT Lashkar-e-Tayyiba (Army of the Righteous).

LTBT Limited (Nuclear) Test Ban Treaty.

LTTE Liberation Tigers of Tamil Eelam.

LVF Loyalist Volunteer Force.

Mach The speed of sound in air (under certain temperature conditions) is called Mach 1. Mach 2 is twice that speed and so on.

MAD Mutually assured destruction (Cold War security and defense policy).

MAE UAV Predator medium altitude endurance unmanned aerial vehicle.

Magic The codename given to the U.S. Navy Combat Intelligence Unit's effort to break the JN-25 Japanese code during World War II.

Magic chips Micro array of gel-immobilized compounds.

MAGIS Marine Air-Ground Intelligence System.

Magnitude The size of an earthquake, typically reported using the Richter scale. As originally defined by Richter, the magnitude of an earthquake is the logarithm of the amplitude of the largest seismic wave recorded on a particular kind of seismometer located 100 km from the earthquake epicenter. Seismologists today use a variety of magnitude scales that produce similar, but not identical, estimates of earthquake size.

Mail sanitization The process in which mail is decontaminated. The process of mail sanitization can be applied as a precautionary measure to kill micro-organisms that may be contained in the mail or to sterilize mail that is known to be contaminated with dangerous microorganisms.

MALDI-MS Matrix-assisted laser desorption/ionization mass spectrometry.

Malicious data Data that, when introduced to a computer—usually by an operator unaware that he or she is doing so—will cause the computer to perform actions undesirable to the computer's owner. It often takes the form of input to a computer application such as a word-processing or data spreadsheet program. It is thus, distinguished from a malicious program such as a computer virus, compared to which malicious data is perhaps even more stealthy.

Manhattan Project The Manhattan Project (officially the Manhattan Engineer District) was a secret, World War II effort by the United States to design and build the world's first nuclear weapon. Commanding the efforts of the world's greatest physicists and mathematicians during World War II, the $20 billion project resulted in the production of the first uranium and plutonium bombs. The American quest for nuclear explosives was driven by the fear that Hitler's Germany would invent them first and thereby gain a decisive military advantage.

Mapping Technology A broad term that describes the equipment and techniques used to prepare, analyze, and distribute maps of all kinds.

Marshall Plan American economic aid program designed to facilitate the reconstruction of Western Europe after World War II.

MARV Miniature autonomous robotic vehicle.

MASINT Measurement and signature intelligence. The term refers to forms of information gathered by means other than through the traditional ones, which include analysis of signals (SIGINT), imagery (IMINT), or data acquired through human contact (HUMINT). MASINT includes acoustic intelligence (ACINT), infrared intelligence (IRINT), laser intelligence (LASINT), nuclear intelligence (NUCINT), optical intelligence (OPINT), and unintentional radiation intelligence (RINT).

Mass spectrometry Separation of ions in a magnetic field according to their masses.

MAV Micro-air vehicle.

MAXI Modular Architecture for eXchange of Intelligence.

McCarthyism Period of anti-communist fervor in American politics in late 1940s and early 1950s; taken from the name of its chief proponent, U.S. Senator Joseph McCarthy of Wisconsin.

MCGPS Mapping, Chart, and Graphics Production System.

MCI United States Marine Corps Intelligence.

Measurement and signatures intelligence (MASINT) Information gathered by analysis of signals (SIGINT), imagery (IMINT), or data acquired through human contact (HUMINT).

MEK Mujahedin-e Khalq Organization (MEK of MKO).

Meltdown A nuclear power plant accident in which the molten uranium of the ruined core will coalesce into a single superheated mass and melt its way down to the groundwater below the plant, causing a violent steam explosion and dispersing even larger quantities of radioactive material. Also known as the China Syndrome.

MEMS Microelectromechanical systems.

MERIT Military exploitation of reconnaissance and intelligence technology.

MGB USSR Ministry of State Security.

MI5 (British Security Service) Best known by its designation as MI5, the Security Service is the leading counterespionage agency working in the United Kingdom. Its functions are somewhat akin to those of the United States Federal Bureau of Investigation, but MI5 places a much greater emphasis on intelligence, and its operatives have no arrest powers.

MI6 (British Secret Intelligence Service) Officially known as the Secret Intelligence Service (SIS), MI6 is the chief British foreign intelligence organization, analogous to the United States Central Intelligence Agency.

MIC Maritime Intelligence Center.

Microchannel In an light amplification device, a narrow cylinder of biased semiconductor that amplifies electron flow.

Microchip Microchips, also termed "integrated circuits" or "chips," are small, thin rectangles of a crystalline semiconductor, usually silicon, that have been inlaid and overlaid with microscopically patterned substances so as to produce transistors and other electronic components on its surface.

Microdot A miniature photograph less than 1mm in diameter.

Microfilm Miniature films used for photographing objects and documents. The images on these films cannot be seen without an optical aid, either in a form of a magnifying glass or a projector.

Microphones A transducer converting the sound waves into electrical signals proportional to the strength of the sound. The microphone output can be recorded or transmitted.

Microsat Generally defined as a satellite weighing between 22.2 lbs to 222 lbs (10 to 100 kg).

MIGS Multi-Source Intelligence Ground System.

MIIDS Military Intelligence Integrated Data System.

Minisat Generally defined as a satellite weighing between 220 lbs to 2200 lbs (100 to 1000 kg).

MINS Multisource Integrated Notification System.

MINT Multi-Source Intelligence Tools.

MKO Mujahedin-e Khalq Organization.

MMWR CDC's Morbidity and Mortality Weekly Report.

MOAB In addition to its raw destructive power, the Massive Ordinance Air Burst bomb (MOAB) has became part of a military and intelligence effort to discourage and demoralize enemy forces. Upon detonation, MOAB produces a mushroom cloud similar to a nuclear blast. The MOAB bomb is the most powerful non-nuclear weapon in the U.S. arsenal.

Moderator Substance that separates fuel elements in a nuclear reactor, slowing down neutrons to increase the likelihood that they will cause further fission events.

Mole An agent who has infiltrated an enemy's intelligence organization.

Money laundering Hiding the profits earned from criminal activities by converting them into a different type of currency or asset, or by moving them to a secretive place.

Mossad Israeli Institute for Intelligence and Special Tasks.

MP Military police.

MPAS Measurement and signature intelligence analysis.

MPC&A Materials Protection, Control, and Accounting, NNSA.

MRTA Tupac Amaru Revolutionary Movement.

MT Machine translation.

Multisensory grenades Grenades emitting disorienting light flashes, painfully loud sounds, and possibly disagreeable odors.

Multispectral An adjective describing a sensor that is able to record signals in more than one band of electromagnetic wavelengths, or an image produced using such a sensor.

MUSIC Multi-User Special Intelligence Communications System [NAVSECGRU].

Mustard gas A substance used in chemical warfare. It is the popular name for the compound with the chemical designation 1,1-thiobis(2-chloroethane) (chemical formula: Cl-CH2-CH2-S-CH2-CH2-Cl). Mustard gas has a number of other names by which it has been known over the years, including H, yprite, sulfur mustard and Kampstoff Lost.

MW Molecular weight.

NACDF National Area Coverage Data Files.

NACIC National Counter Intelligence Center.

NAILS The National Automated Immigration Lookout System (NAILS) is a centralized database and computing system used by entry inspectors to identify aliens not eligible for admission.

NALU National Army for the Liberation of Uganda.

Nanosat Generally defined as a satellite weighing between 2.2 lbs. and 22 lbs. (1 to 10 kg).

Nanotechnology Device components ranging in size between 1/10,000,000 (one ten millionth of a millimeter) and 1/10,0000 millimeter.

NAPP National Aerial Photography Program.

NARA National Archives and Records Administration.

NARAC United States National Atmospheric Release Advisory Center.

Narcoanalysis A psychotherapeutic method which uses a sedative or hypnotic drug as an aid to compel patients to speak without inhibition.

Narcoterrorism Terrorism undertaken by groups directly or indirectly involved in producing, transporting, or distributing illegal drugs.

NAS National Academy of Science.

NASA National Aeronautics and Space Administration.

National command authorities Within a national government, the national command authorities are the persons or officeholders (or their duly deputized alternates or successors) who have the legal power to direct military activities.

National Intelligence Estimate(NIEs) Reports by the National Intelligence Council (NIC), drawing on estimative views from across the Intelligence Community.

NATO North Atlantic Treaty Organization.

NCA National Command Authority.

NCIC National Crime Information Center.

NCIS Navy Criminal Investigative Service.

NCIX National Counterintelligence Center (NACIC), the U.S. Office of the National Counterintelligence Executive (NCIX) was created early in the twenty-first century. It educates members of government organizations and the private sector on the need to maintain vigilance against espionage, both political/national and economic/industrial. NCIX conducts regional seminars, issues publications, and produces other materials.

NCLIS United States National Commission on Libraries and Information Science.

NCR National Council of Resistance.

NCS National Communications System.

NDIC Department of Justice National Drug Intelligence Center.

NDPO Domestic Preparedness Office, United States National.

NDTA National Drug Threat Assessment.

Need to know A demonstrable and recognized purpose for accessing specific information.

NERSC National Energy Research Scientific Computing Center.

Nerve gas Nerve gases, or nerve agents, are mostly odorless compounds belonging to the organophosphate family of chemicals that inhibit the enzyme acetylcholinesterase and disrupt the transmission of nerve impulses in the body.

NES NIMA/National Exploitation System.

NEST team Nuclear Emergency Support Team.

Network A group of computers linked by communication lines.

Network A group of individuals or cells (subgroups) engaged in specific operations (e.g., espionage or terrorist operations).

Neurotranmitter A chemical that functions to pass a nervous impulse chemically through the synapse (gap) separating neurons (nerve cells).

NFIB The National Foreign Intelligence Board (NFIB) was created by the National Security Act of 1947. The NFIB acts as a communications channel among various national intelligence agencies and facilitates interagency exchange of information. The board also develops policy regarding the protection of intelligence information.

NFIP The National Foreign Intelligence Program, an annual budget request for the Intelligence Community, presented to the President of the United States by the Director of Central Intelligence.

NGP Non-governmental organization.

NHAP National High Altitude Photography Program.

NI Naval Intelligence.

NIC National Intelligence Council.

NIF National Ignition Facility.

Night scopes Infra-red scopes. Night vision scopes are devices that enable machines or people to "see in the dark," that is, to form images when illumination in the visible band of the electromagnetic spectrum is inadequate.

NIH National Institutes of Health.

NIJ National Institute of Justice.

NIM United Kingdom National Intelligence Machinery.

NIMA National Imagery and Mapping Agency.

NIPC National Infrastructure Protection Center.

NIPR Revolutionary Proletarian Initiative Nuclei.

NIPRNET Non-Classified Internet Protocol Router Network.

NIS Navy Criminal Investigative Service.

NISAC National Infrastructure Simulation and Analysis Center.

NIST The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency under the aegis of the Undersecretary for Technology in the U.S. Department of Commerce. It is concerned with maintaining measurement and calibration standards, including those related to a number of Homeland Security projects and agencies.

NITFS National Imagery Transmission Format.

NIWA Naval Information Warfare Activity.

NKVD USSR People's Commissariat of Internal Affairs.

NLA The National Liberation Army of Iran.

NMD National Missile Defense.

NMIC The National Maritime Intelligence Center (NMIC) brings together intelligence operations for the United States: Navy, Marine Corps, and Coast Guard.

NMJIC United States National Military Joint Intelligence Center.

NMR Nuclear magnetic resonance.

NNSA National Nuclear Security Administration.

Nonpersistent chemical warfare agent Chemical warfare agents that maintain toxicity for a brief time (or until dispersed by weather).

NORAD The North American Air Defense Agreement, signed on May 12, 1958, by the United States and Canada, created a continental air defense warning and surveillance system in response to Cold War fears of an airborne attack by the Soviet Union. The resulting North American Air/Aerospace Defense Command (NORAD) has since shifted strategies from guarding against long-range bombers to warning of ballistic missile attacks and maintaining space surveillance.

NPA New People's Army.

NPIC National Photographic Interpretation Center.

NPT Non-Proliferation Treaty (nuclear weapons).

NQR Nuclear quadrupole resonance.

NRC Nuclear Regulatory Commission.

NRIIS National Radar Imagery Interpretation Standard.

NRO National Reconnaissance Office.

NRT National Response Team.

NRTD Near real time dissemination.

NS/EP National security and emergency preparedness.

NSA The National Security Agency (NSA) is the leading cryptologic organization in the United States intelligence community. Focused on cryptologic and cryptanalytic missions, it is the nation's leading employer of mathematicians.

NSC National Security Council, the U.S. president's Intelligence Advisory Council.

NSD National Signal Databases.

NSF National Science Foundation.

NSOC National SIGINT Operations Center.

NTA Anti-Imperialist Territorial Nuclei.

NTSB National Transportation Safety Board.

NTTC National Technology Transfer Center (Emergency Response Technology Program).

Nuclear Emergency Support Team (NEST) An emergency response asset of the National Nuclear Security Administration (NNSA).

Nuclear reactors Complex devices in which fissionable elements such as uranium, thorium, or plutonium are made to undergo a sustainable nuclear chain reaction. This chain reaction releases energy in the form of radiation that (a) sustains the chain reaction; (b) transmutes (i.e., alters the nuclear characteristics of) nearby atoms, including the nuclear fuel itself; and (c) may be harvested as heat.

Nuclear spectroscopy A powerful tool in the arsenal of scientists and forensic investigators because it allows detailed study of the structure of matter based upon the reactions that take place in excited atomic nuclei.

Nuclear weapons Explosive devices that utilize the processes of fission and fusion to release nuclear energy.

Nucleic acid analyzer (HANAA) HANAA is an acronym for the hand-held advanced nucleic acid analyzer. HANAA is a real time polymerase chain reaction (PCR) based system for detecting pathogens (disease-causing organisms).

Nuclide A type of atom having a specific number of protons and neutrons in its nucleus.

OAR Office of Air and Radiation.

OARS Outlying Area Reporting Station.

OASIS Over-the-Horizon (OTH) Airborne Sensor Information System (OASIS).

Observable Any form of energy radiated by an object, such as an aircraft, that might be observed by an opponent.

OEM Office of Emergency Management.

OER Office of Emergency Response, United States Department of Energy (DOE).

OERR Office of Emergency and Remedial Response. An administrative office of the Environmental Protection Agency (EPA) in charge of administering the Superfund Program and initial responses to environmental crises.

OFAC United States Office of Foreign Asset Control.

Official Secrets Act, United Kingdom The Official Secrets Act of the United Kingdom prohibits the transfer of information deemed sensitive to national security interests.

OGC United States Offices of Global Communications.

OGPU USSR Unified State Political Directorate.

OIG United States Office of the Inspector General.

OILSTOCK NSA Geographic Information System.

OIPR United States Office of Intelligence Policy and Review.

OIS United States Office of Information Security.

OIW Ops/Intel Workstation.

Oligonucleotide A chemically synthesized short single-stranded DNA molecule.

One-time pad A cipher pad intended to be used for the encipherment and decipherment of a single message.

ONI Office of Naval Intelligence.

ONR Office of Naval Research.

OPEC Organization of Petroleum Exporting Countries, a cartel controlling much of the world's petroleum production.

Open code Communicating openly, but with the use of references with significant meaning to the recipient.

Open sources Non-classified sources that include such sources as official statistical publications, newspapers, radio broadcasts, and trade publications.

Operational intelligence Intelligence involved in military planning for a particular theatre or area of operations.

Operative An employee of an intelligence agency. Compare with *agent* and *intelligence officer.*

ORNL Oak Ridge National Laboratory.

OSIS Open Source Information System.

OSIS Ocean Surveillance Information System.

OSS Office of Strategic Services, forerunner of the CIA.

OV Orange Volunteers.

Overflight A mission by a spy plane over an enemy country to collect intelligence using electronic or photographic equipment.

Overt information Information gathered from published sources.

P-3 P-3 Orion anti-submarine maritime reconnaissance aircraft.

PAGAD People Against Gangersterism and Drugs.

PAM Payload assist module.

Parabolic microphone A microphone inside a dish, able to pick up sounds from a distance.

Parallel processing The use of two or more computers working in tandem to solve a problem.

Paroles Key words or signals used to establish mutual identification.

PARSEC SIGINT Analysis and Reporting software.

Passive SONAR A sensitive listening-only SONAR mode to detect presence of objects making noise.

Pathogen Genomic Sequencing The Pathogen Genomic Sequencing program focuses on characterizing the genetic components of pathogens in order to develop novel diagnostics, treatments and therapies for the diseases they cause.

Pathogens Organisms, frequently microorganisms, or components of these organisms, that cause disease. Many diseases caused by microbial pathogens, and the frequency of these diseases, are a national security issue.

Patroit act The Patriot Act, or Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Public Law 107–56), was signed into law on October 26, 2001, in the wake of terrorist attacks on the World Trade Center and Pentagon. The law grants law enforcement and intelligence agencies more power to detain and question suspects for longer periods of time, and increases their ability to conduct surveillance operations.

Patriot missile system An advanced ground-based air defense system.

Payload An object that is delivered by a missile or other rocket.

P-band 0.230–1.000 GHz.

PCR The polymerase chain reaction (PCR), refers to a widely used technique in molecular biology involving the amplification of specific sequences of genomic DNA, the genetic material found in virtually all living cells.

Penetrability The ease with which soil, rock, concrete, or other material can be penetrated by projectiles or other earth penetrating weapons.

Penicillin The first antibiotic. Discovered by Sir Alexander Fleming, it is produced by a species of a mold microorganism.

Perigee An orbital position were a satellite is closest to Earth.

Persistent chemical warfare agent Chemical warfare agents that maintain toxicity for a prolonged period (usually several days).

PET Positron emission tomography.

PFIAB The President's Foreign Intelligence Advisory Board (PFIAB) provides unbiased monitoring of the overall intelligence effort of the United States by continually reviewing the activities of agencies and departments engaged in intelligence work.

PFLP Popular Front for the Liberation of Palestine.

PFLP-GC Popular Front for the Liberation of Palestine-General Command.

PGP Pretty Good Privacy, an encryption program.

Photographic Interpretation Center The Central Intelligence Agency (CIA) established the National Photographic Interpretation Center (NPIC) in the 1950s to provide skilled interpretation of photographic images obtained by low- and high-flying aircraft, and later by satellites. In 1973 the NPIC, originally a unit of the CIA Directorate of Intelligence, transferred to the Directorate of Science and Technology (DS&T). In 1996, it was moved to the newly formed National Imagery and Mapping Agency (NIMA).

Photographic resolution The term *resolution,* in the context of photography, refers to the degree to which adjacent objects can be distinguished from one another in a photographic image.

PHS Public Health Service.

PIADC Plum Island Animal Disease Center.

PIC Pressurized ionization chamber.

Picosat Generally defined as a satellite weighing less than 2.2 lbs (1 kg).

PIDS Perimeter Intrusion Detection System.

PIJ Palestine Islamic Jihad.

PINES Pacific Air Forces Interim National Exploitation System.

PIRA Provisional Irish Republican Army.

PKK Kurdistan Workers' Party (PKK).

Plaintext A message in ordinary language that is to be enciphered.

Playfair cipher The Playfair cipher is a method of cryptography invented in 1854 by English physicist Sir Charles Wheatstone (1802–1875).

PLF Palestine Liberation Front.

PLO Palestine Liberation Organization.

Plum Island Animal Disease Center (PIADC) The PIADC, located on a 180 acre site off the northeastern tip of Long Island, New York, is part of the Department of Homeland Security's efforts to protect the United States's food supply. PIADC efforts work to protect U.S. consumers and safeguard the integrity of U.S. animal product exports against catastrophic economic losses caused by biologic agents accidentally or deliberately introduced by terrorists.

PMOI People's Mujahidin of Iran.

PNG Pseudorandom number generator.

P-note A counterfeit banknote produced with a computer printer.

POG Hizballah (Party of God).

Polarization Plane of vibration of an electrical signal (the orientation of a signal's electrical field).

Politburo The central policy-making and governing body of the USSR Communist Party.

Polybius square A grid in which letters of the alphabet are arranged in a square such that each letter has a unique position identifiable by the numbers of its row and column.

PORTPASS The Port Passenger Accelerated Service System (PORTPASS) is a generic term for programs developed to expedite passage through U.S. national entry systems. PORTPASS components include the INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System), SENTRI (Secure Electronic Network for Travelers' Rapid Inspection), OARS (Outlying Area Reporting Station), and RVIS (Remote Video Inspection System) systems.

POTUS President of the United States.

Power For many electronic devices this term denotes power required or consumed by operation. Often, however, the term "power" denotes a specialized contextual or application-related meaning (e.g., with regard to a signal transponder it commonly refers to signal amplification power).

PRC People's Republic of China.

Presidential directive A classified set of guidelines or rules issued by the President of the United States, usually in reference to some sensitive issue such as security or intelligence.

Primary RADAR RADAR systems that receive reflections of their own transmitted signals as returned signals from the target.

Principal agent An agent who performs the role of surrogate handler, working over other agents and reporting to an intelligence officer.

Profiling The process of developing descriptions of the traits and characteristics of unknown offenders in specific criminal cases.

Propaganda A form of communication that attempts to influence the behavior of people by affecting their perceptions, attitudes and opinions.

Propagation Traveling or penetration of waves through a medium.

Prophylaxis Pre-exposure treatments (e.g., immunization) that prevents or reduces severity of disease or symptoms upon exposure to the causative agent.

Protein Macromolecules made up of long sequences of amino acids.

Pseudoscience (false science) Arguments or ideas, often laced with scientific terminology or bizarre calculations, based on theories developed outside of the scientific method and thus not subject to scientific validation.

PSI Personnel security investigation.

Psychological warfare The use of tools and techniques designed to influence the views of allies, enemies, and neutrals. Propaganda is a major component of psychological warfare, which includes other facets such as displays of force, and contrasting positive and negative treatment of detainees—known colloquially as "good cop/bad cop."

Psychotropic drugs A loosely defined grouping of agents that have effects on psychological function and include antidepressants, hallucinogens, and tranquilizers. They are all compounds that affect the functioning of the mind through pharmacological action on the central nervous system.

Public Health Service, United States A federal government agency that promotes the health of the people of the United States and the world. It is a principle component of the Department of Health and Human Services (HHS) and is composed of eight agencies. Among other duties, the Public Health Service is charged with, through its agencies, preparing for and leading the nation's medical response to a threat or disaster, whether naturally occurring or an act of terrorism.

Public key cipher Cipher system which allows the exchange of enciphered messages without prior distribution of secret keys to all users. Each user calculates their own secret key and uses it in combination with a public key to send and receive messages.

Purple Machine An Allied codename for one of several Japanese cipher machines used during World War II.

Puzzle Palace Nickname for the NSA (United States National Security Agency).

QuIST Quantum Information Science and Technology.

Radar Radar—an acronym for *RA*dio *D*etection *A*nd *R*anging—is the use of electromagnetic waves at sub-optical frequencies (i.e., less than about 10^{12} Hz) to sense objects at a distance.

RADAR, synthetic ap Synthetic aperture RADAR (SAR) is used for high-resolution mapping of the ground from moving aircraft or spacecraft.

RADINT Radar intelligence from nonimaging radar. Unlike ELINT, RADINT does not involve the interception of radar signals; instead, intelligence regarding flight path and other specifics is derived from the deflection of enemy radar signals. RADINT is a subcategory of MASINT, or measurement and signatures intelligence.

Radio frequency (RF) weapons RF weapons, also known as directed-energy weapons, use electromagnetic energy on specific frequencies to disable electronic systems. The principle is similar to that of high-power microwave (HPM) weapons, only HPM systems tend to be much more sophisticated, and are thus, more likely to be in the control of superpowers or near-superpowers. RF weapons, by contrast, are simple and low-voltage enough that they could be deployed by smaller, less technologically enhanced forces.

Radiological Having to do with nuclear radiation.

Radiomimetic An agent or exposure protocol that simulates radioactive exposure.

RAID Real-time Analytical Intelligence Database.

RASCAL Responsive Access, Small Cargo, Affordable Launch.

RCS Radar Cross Section.

RDD Radiological dispersal device, often called a "dirty bomb."

Recombinant DNA DNA that is cut using specific enzymes so that a gene or DNA sequence can be inserted.

Reconnaissance A term for efforts to gain information about an enemy, usually conducted before, or in service to, a larger operation.

Red code A Japanese naval code created during World War I and used until the outbreak of World War II. The Red code used the additive encryption method.

Red Scare Period of anticommunist hysteria in United States from 1918–1920, culminating in the Palmer Raids; also invoked to describe the resumption of anticommunist activities in the late 1940s and early 1950s.

Redoubled agent A double agent whose activities have been discovered by the agency against which he or she is spying, and who is then used—either wittingly or unwittingly, willingly or unwillingly—in that agency's service against the other.

Refractive index (characteristic of a medium) Degree to which a wave is refracted, or bent.

Remote sensing The acquisition of information about an object or phenomenon by a device located a considerable distance from the object or phenomenon.

Resolution The ability of a sensor to detect objects of a specified size. The resolution of a satellite sensor or the images that it produces refers to the smallest object that can be detected.

Retina and iris scans Scans that detect and map the neural part of the eye responsible for vision. The pattern of blood vessels serving the retina is as unique as fingerprints.

RF Radio frequency.

RF detection RF, or radio frequency systems are directed-energy weapons that use electromagnetic energy on specific frequencies to disable electronic systems.

RF weapons Radio frequency weapons, also known as directed-energy weapons, which use electromagnetic energy on specific frequencies to disable electronic systems.

RHD Red Hand Defenders.

Richter scale Scale used to measure the intensity of seismic events, or earthquakes.

Ricin A highly toxic protein that is derived from the bean of the castor plant (*Ricinus communis*). The toxin causes cell death by inactivating ribosomes, which are responsible for protein synthesis. Ricin can be produced in a liquid, crystal or powdered forms and it can be inhaled, ingested, or injected. It causes fever, cough, weakness, abdominal pain, vomiting, diarrhea, dehydration, and death. There is no cure for ricin poisoning.

Ring A group or network.

RIRA Real IRA.

RJO Revolutionary Justice Organization.

RN group (Greece) Revolutionary Nuclei.

RNA Ribonucleic acid.

Rogue state A nation that harbors terrorists and poses a serious security threat to its neighbors.

RPA Revolutionary Proletarian Army.

RTH Radioactive thermoelectric generators.

RUF Revolutionary United Front.

RVIS Remote Video Inspection System.

S&T Directorate of Science and Technology (S & T), Department of Homeland Security.

Sabotage A deliberate act of destruction or work stoppage intended to undermine the activities of a larger entity, whether it is a business, government, or some other organization. The practice of sabotage, which has roots in the labor movements of the late nineteenth and early twentieth centuries, gained military and political application during the world wars and thereafter. It has also been a part of covert operations, often undertaken by agents provocateur.

Safe house Any precleared or secret building where agents can meet or operate without detection.

SAIP Semi-Automatic IMINT Processing Systems.

SANDKEY NSA Analysis and Reporting software.

Sanitize To delete sensitive or classified information prior to release.

SAR Search and rescue.

SAR Synthetic Aperture Radar.

Sarin gas Sarin gas (O-Isopropyl methylphosphonofluoridate), also called GB, is a dangerous and toxic chemical. It belongs to a class of chemical weapons known as nerve agents, all of which are organophosphates. The G nerve agents, including tabun, sarin and soman, are all extremely toxic, but not very persistent in the environment. Pure sarin is a colorless and odorless gas, and since it is extremely volatile, can spread quickly through the air.

SARS Severe Acute Respiratory Syndrome.

S-band 2.700–3.500 GHz.

SBCCOM United States Army Soldier and Biological Chemical Command.

SB-WASS Space Based Wide Area Surveillance.

Scalable The degree to which an algorithm is capable of implementing additional computational resources in such a way as to solve increasingly more complex problems. To be truly scalable, the work required to solve an algorithm should grow at a rate smaller than the rate at which the amount of input grows.

Scientific intelligence Intelligence on the development of new weapons or techniques by an enemy. Closely related to TECHINT, or technical intelligence.

SDI Strategic Defense Initiative.

SDNS Secure Data Network System [NSA].

SDS Surveillance Direction System.

SEAL teams U.S. Navy Sea-Air-Land (SEAL) Teams (special forces).

SEASAT Ocean surveillance satellite.

Secret The second highest U.S. general security classification. A term referring both to information whose disclosure to unauthorized personnel could reasonably be expected to cause serious damage to national security, and to the security clearance necessary to access such information.

Secret agent An agent who works in a clandestine capacity, such that the relationship with the intelligence agency is not obvious to those around him or her. Also known as an undercover agent.

Secret writing Any means of written communication whereby a spy conceals the actual written text, whether it be enciphered/encoded or not. Codes and ciphers are sometimes mistakenly placed under the heading of "secret writing," but this is accurate only if that expression is taken in its most general sense, as writings that are concealed in any way. Whereas codes and ciphers conceal the meaning of a message, secret writing conceals the actual message.

Security clearance A limited license or initial general permission to access classified information—that is, any data or material belonging to the federal government that relates to sensitive topics such as military plans or vulnerabilities of security systems.

Sedret Spoke An Echelon security compartment equivalent to the general security level designation "Confidential."

Seismogram The visual record of earthquake vibrations or waves produced by a seismograph, which is an instrument capable of sensing and recording the waves.

Seismograph An instrument that measures and records elastic ground vibrations called seismic waves that are generated by earthquakes and man-made explosions. Seismology has been an important tool for the remote detection of large explosions, especially underground nuclear tests, for many years and is expected to play an important role in Comprehensive Test Ban Treaty verification.

Sendero Luminoso Shining Path, or SL.

Sensitive Compartment Information (SCI) Data concerning sophisticated technical systems for collecting intelligence, as well as information collected by those systems, access to which requires a special security clearance.

SENTRI Secure Electronic Network for Travelers' Rapid Inspection.

SF 86 Standard Form 86, a "Questionnaire for National Security Positions" that federal employees, military personnel, and contractors must complete in order to gain a security clearance.

SFAI Swept Frequency Acoustic Interferometer.

Shin Bet The Israeli intelligence agency.

Shin Beth The Israeli counterintelligence service.

Shining Path Sendero Luminoso (Shining Path, or SL).

Short wave Radio frequencies ranging from the upper limit of the AM band to the lower limit of the VHF (television) band (1605 kHz to 54 MHz).

Short-wave transmissions Radio transmissions in the range somewhere between 2 and 30 MHz (megahertz, or million cycles per second). Because these signals are capable or propagating over a greater distance than either AM or FM radio, shortwave is the preferred medium for radio broadcasting to remote locations.

SIDR Secure Intelligence Data Repository.

SIGINT Signals intelligence, or intelligence derived from the interception of signals, including communications signals, electronic emissions, and telemetry. The two major subsets of SIGINT are COMINT or communications intelligence, and ELINT or electronics intelligence. SIGINT, is one of the four major forms of intelligence, along with human, imagery, and measurement and signatures intelligence (HUMINT, IMINT, and MASINT respectively).

Signature In the MASINT context, *signature* refers to characteristic markings, such as the auditory signature of a submarine detected on sonar.

Silencer A device contrived to suppress sound by means of an attachment to a firearm.

SIPRNET Secret Internet Protocol Router Network.

SIS Signal Intelligence Service, the U.S. Army group responsible for deciphering Japanese diplomatic codes during World War II.

Skunk Works The nickname for the headquarters of advanced development programs for Lockheed Martin Aeronautics Company at Palmdale, California, some 80 miles (128 km) north of Los Angeles in the Antelope Valley. Established in 1943 by what was then known as the Lockheed Aircraft Corporation, the Skunk Works has been the birthplace of numerous extraordinary aircraft, including the U-2 and SR-71 reconnaissance planes, and the F-117A stealth fighter.

SL Sendero Luminoso (Shining Path, or SL).

SLBM Submarine-launched ballistic missile.

Sleeper agent An agent placed in an undercover situation and told to await further instructions before beginning to actively engage in espionage activities. A sleeper may remain inactive for months or years, or even the rest of his or her life.

Smallpox An infection caused by the variola virus, a member of the poxvirus family. The disease is highly infectious. Passage from person to person via contaminated aerosolized droplets (from sneezing, for example) occurs easily, and so the spread of smallpox through a population can occur quickly.

Smart card A card with biometric and other data contained in an embedded microchip or other form of integrated circuitry.

SMERSH A KGB assassination team (*SMERrt SHpionam* or "Death to Spies").

SMPAS Space Mission Payload Assessment System.

SOE Special Operations Executive.

SOF-IV Special Operations Forces—Intelligence Vehicle.

Solid phase microextraction techniques (SPME) A chemical technique designed to detect chemical compounds. In its forensic application, it is used to find chemical warfare agents, high explosives, or illegal drugs.

Soman Soman (or "GD") is a synthetic (human-made) compound that affects the functioning of nerves. As such, soman is one of a group of chemicals (e.g., tabun) that are known as nerve agents.

SONAR Sound Navigation and Ranging (SONAR) is a remote sensing system with important military, scientific and commercial applications. Active SONAR transmits acoustic (i.e., sound) waves. Passive SONAR is a listening mode to detect

noise generated from targets. SONAR allows the determination of important properties and attributes of the target (i.e., shape, size, speed, distance, etc.).

SOSUS Sound Surveillance System.

Special agent A term for operatives of the Federal Bureau of Investigation (FBI) during the leadership of J. Edgar Hoover and thereafter. By this designation, Hoover meant to distinguish FBI agents from ordinary police officers.

Special Operations Executive (SOE) The British Special Operations Executive, created in 1940, was given the mission to "set Europe ablaze." The SOE supplied and organized resistance cells in Nazi-occupied Europe, carrying out missions of intelligence gathering, sabotage, and other covert activities.

Special relationship During World War II, the intelligence services of the United States and the United Kingdom worked together in their efforts against the Axis powers, particularly in Europe, and formalized the collaboration with agreements in 1943 and 1946.

Spectra Low-frequency collection system used by the Navy.

Spectroscopy The measurement of the absorption, scattering or emission of electromagnetic radiation by atoms or molecules.

Spook An American term for an intelligence officer or agent.

Spore A hard casing that contains the genetic material of those bacteria and other microorganisms that are able to form the structure. This physically and chemically resilient package protects the genetic material during periods when the environmental conditions are so harsh that the growing form of the microbe would be killed.

SPOT A French satellite, *System Probetoire d'Observation de la Terre*.

SPR Strategic Petroleum Reserve.

Spread spectrum A radio signal spread out across a range of frequencies to evade detection and decoding.

SR-71 A SR-71 spy plane is a black-colored, high-altitude airborne reconnaissance platform.

SSA Signal Security Agency.

SSCI United States Senate Select Committee on Intelligence.

SST Space Surveillance Telescope.

START Strategic Arms Reduction Treaty.

Stasi The *Ministerium für Staatssicherheit*, Ministry of State Security, was the primary intelligence and security agency of the German Democratic Republic (GDR), or East Germany, during the cold war.

Static address A permanent Internet protocol (IP) address that uniquely identifies a computer connected to the Internet.

StB (Statni Bezpecnost) The "secret police" of Czechoslovakia before 1990.

Stealth technology Stealth technology, also termed "low-observable" technology, is a set of techniques that render military vehicles, mostly aircraft, hard to observe. Because RADAR—an acronym for *RA*dio *D*etection *A*nd *R*anging—is the primary detection technology for aircraft, most stealth technologies are directed at suppressing RADAR returns from and infrared observation of aircraft.

Steganography (from the Greek for "covered writing"). The secret transmission of a message. It is distinct from encryption, because the goal of encryption is to make a message difficult to read while the goal of steganography is to make a message altogether invisible.

STICS Scalable Transportable Intelligence Communications System [NSA].

Stinger A nickname for two very different weapons. The first, a 22-caliber pistol that could be hidden in a toothpaste tube, was used by the CIA after World War II. The second, developed by General Dynamics in the 1970s, was a surface-to-air missile used most notably by Afghan *mujahideen* against the Soviets in the 1980s.

Strategic Arms Limitation Treaty (SALT) A series of treaties begun in 1972 that limited the number of long-range offensive missiles held by the United States and the Soviet Union.

Strategic geologic intelligence The geologic or geotechnical information necessary to evaluate the vulnerability of an underground facility to attack.

Strategic metal A metal that is essential for industry and national security, but for which a nation has little or no domestic supply. The ores of strategic metals are often referred to as strategic minerals.

Strategic Petroleum Reserve (SPR) The SPR, located in the United States and operated by the Department of Energy (DOE), is the largest emergency supply system of oil in the world.

Stream cipher Stream ciphers operate upon a series of binary digits ("bits," usually symbolized as 1s and 0s), enciphering them one by one rather than in blocks of fixed length.

Stringer A freelance agent who works periodically or occasionally for an intelligence agency.

Strong encryption A method of encryption in which a cipher is unbreakable, or virtually unbreakable, without knowledge of the key.

Suitcase bomb A small, portable nuclear weapon, usually weighing less than 100 pounds, that can be transported and hidden in a suitcase or other small container.

Superfund Program Established by the United States Congress in 1980 to locate, investigate, and clean up the worst toxic waste sites nationwide.

Supreme Truth Aum Supreme Truth (Aum) Aum Shinrikyo, Aleph.

Surveillance Intelligence-gathering observations made regularly or continuously in order to monitor an area of interest for changes.

SVR Russian foreign intelligence.

SZ42 cipher machine A cipher machine used by Germany in WWII. The German military did not replace Enigma with the SZ42 for general use because the SZ42's complexity made it too heavy for the field.

Tabun Tabun (or "GA",O-ethyl N,N-dimethylphosphoroamidocyanidate) is one of a group of synthetic chemicals that

were developed in Germany during the 1930s and 1940s (tabun was developed in 1936). The original intent of these compounds, including tabun, was to control insects. However, tabun and the other human-made nerve agents proved to be much more potent than the organophosphates, and so quickly became attractive as chemical weapons.

Tapping The clandestine physical interception of electronic messages, especially telephone conversations and messages.

Targeting The prioritization of certain target areas or facilities for possible military or intelligence action.

TECHINT Technical intelligence, or intelligence relating to the technical abilities of an enemy. TECHINT does not fall under just one of the four major branches of intelligence; rather, it includes elements of imagery, measurement and signatures, and signals intelligence (IMINT, MASINT, and SIGINT respectively).

TECS Treasury Enforcement Communication System.

Telemetry The process of making measurements from a remote location and transmitting those measurements to receiving equipment.

TELINT Telemetry intelligence, an example of which is the use of signals to relay information on the performance of a guided missile system. TELINT is a subset of FISINT (foreign instrumentation signals intelligence), which is in turn a subcategory of ELINT, or electronic intelligence.

TERPES Tactical Electronic Reconnaissance Processing and Evaluation System.

Terrorism The systematic belief in the political, religious, or ideological efficacy of producing fear by attacking—or threatening to attack—unsuspecting or defenseless populations, usually civilians, and usually by surprise.

THAAD Theater High Altitude Area Defense.

Thin layer chromatography Thin layer chromatography, which is typically abbreviated as TLC, is a type of liquid chromatography that can separate chemical compounds of differing structure based on the rate at which they move through a support under defined conditions.

TIA Total Information Awareness.

TIARA Tactical Intelligence and Related Areas, an annual budget request for specific tactical intelligence requirements of the military services, presented by the Secretary of Defense to the President of the United States.

TIFG Tunisian Islamic Fighting Group.

TMD-GBR Theater Missile Defense-Ground Based Radar.

TNT The explosive, trinitrotoluene.

Top Secret The highest general U.S. security classification. Other restrictions include "need to know access." Top secret refers to information whose disclosure to unauthorized personnel could reasonably be expected to cause exceptionally grave damage to national security, and to the security clearance necessary to access such information.

Top Secret Umbra An Echelon security compartment equivalent to the general security level designation "Top Secret."

Topographic map A map reflecting the shape, or topography, of Earth's surface. Topography can be depicted using contour lines of equal elevation or by using shading techniques to simulate a three dimensional surface.

Toxicity The degree to which a chemical, in sufficient exposure, can poison humans or other organisms.

Toxicology The science of toxicology is concerned with the adverse effects of chemicals on biological systems and includes the study of poisons, their detection, action and counteractions. Toxicologists today generally use the techniques of analytical chemistry to detect and identify foreign chemicals in the body, with a particular emphasis on toxic or hazardous substances.

Toxin weapons A poison produced by a living organism, or its derivative.

Tradecraft Techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business.

Transducer An instrument that that converts one type of energy into another.

Transmutation The conversion of one nuclide into another, as by neutron bombardment in a nuclear reactor.

Transponder Integrated operation of receivers, frequency converters, and transmitter devices.

Triangulation A means of navigation and direction finding based on the trigonometric principle that, for any triangle, when one side and two angles are known, the other two sides and triangles can be calculated.

Trojan horse A security-breaking program, disguised as a benign product, that is designed for the purpose of clandestinely introducing itself into a remote user's computer, and then wreaking havoc in one way or another.

Truth drugs Anesthetics employed in interrogation that are intended to act as truth serums.

Truth serum A term given to any of a number of different sedative or hypnotic drugs that are used to induce a person to tell the truth. Truth serums cause a person to become uninhibited and talkative, but they do not guarantee the veracity of the subject.

TSA Transportation Security Administration (previously part of the Department of Transportation). On March 1, 2003, agents were transferred to the Department of Homeland Security (DHS), directorate of Border and Transportation Security (BTS).

Tularemia A plague-like disease caused by the bacterium *Francisella tularensis*.

Typex The name for the principal encryption device, or cipher machine, used by the military, intelligence, and diplomatic services of the British Empire during World War II.

UDA/UVF Ulster Defense Association/Ulster Freedom Fighters (UDA/UVF).

UFO (Unidentified Flying Object) A flying object of unknown origin, popularly but unscientifically assumed to be associated with extraterrestrial beings or paranormal phenomena. Most often, UFOs are explained by weather phenomena or military aircraft.

UHF-band 0.430–1.300 GHz.

Ultra Operation Ultra was the codename for the British cryptologists efforts at Bletchley Park to intercept and break

German coded messages. While Ultra initially was the cryptonym for the project to break the German Enigma machine, the code name came to represent all British efforts to break high-level German radio codes during World War II.

Umbra Gamma An Echelon security compartment equivalent to the general security level designation "Secret."

UN United Nations.

Undercover agent An agent who works in a clandestine capacity, such that the relationship with the intelligence agency is not obvious to those around him or her. Also known as a secret agent.

Unified command principle The idea, which emerged in U.S. military circles during the late 1980s and began to prevail in the early 1990s, that unified or area commanders in chief should direct all U.S. military operations in a given geographic area.

UNMOVIC United Nations Monitoring, Verification and Inspection Commission.

Uplink An Earth to satellite connection or electronic signal path.

Uranium depletion weapons Depleted uranium (DU) munitions are armor-piercing or general-purpose ammunition rounds that are composed, in part, of depleted uranium. Depleted uranium is uranium that has had most of its ^{234}U and ^{235}U removed for use in nuclear power or nuclear weapons, leaving metal that is almost entirely ^{238}U.

Uriticant A compound that produces excessive skin irritation and itching.

USA United States Army.

USAF United States Air Force.

USAMRICD Army Medical Research Institute of Chemical Defense, United States.

USAMRIID United States Army Medical Research Institute of Infectious Diseases. The facility is operated by the Department of Defense and serves as the country's principle laboratory for research into the medical aspects of biological warfare.

USCG United States Coast Guard.

USCSB United States Chemical Safety and Hazard Investigations Board.

USIGS United States Imagery and Geospatial Information Systems Architecture.

USIS United States Imagery System Architecture.

USMC United States Marine Corps.

USN United States Navy.

USOGE United States Office of Government Ethics.

USPS United States Postal Service.

USSR Union of Soviet Socialist Republics.

USSS United States SIGINT System.

USSTRATCOM United States Strategic Command.

UUV Unmanned undersea vehicles.

UVF Ulster Freedom Fighters.

V-agents A group of alkyl esters of S-dialkylamino ethylmethylphosphonothiolic acids that are nerve agents.

Venona The Venona Project was the United States Army's Signal Intelligence Service, and later the National Security Agency's, operation to intercept and decrypt high-level Soviet diplomatic communications.

VERS The Vaccine Event Reporting System is a U.S. vaccine safety surveillance program that is under the direction of the Food and Drug Administration and the Centers for Disease Control and Prevention.

Viruses Nonliving repositories of nucleic acid that require the presence of a living prokaryotic or eukaryotic cell for the replication of the nucleic acid. There are a number of different viruses that challenge the human immune system and that may produce disease in humans. In common, a virus is a small, infectious agent that consists of a core of genetic material (either deoxyribonucleic acid [DNA] or ribonucleic acid [RNA]) surrounded by a shell of protein.

VOA Voice of America.

Vozrozhdeniye Island A Russian island located in the Aral Sea approximately 1,300 miles to the east of Moscow that was used as a bioweapons test facility for the former Soviet Union.

VR Virtual reality.

Vulnerability assessment A test of a system to locate, diagnose, and correct areas of weakness that might make it susceptible in times of crisis, attack, or destabilization.

VX agent VX nerve agent (O-ethyl S-[2-diisoproylaminoethyl] methylphsophonothioate) is an organophosphate. Although it is often called a nerve gas, VX is usually a clear, odorless, tasteless liquid. A tiny amount of VX, about 10 mg, absorbed through the skin, eyes, or ingested is fatal, and death usually occurs within an hour of exposure.

WAN Wide Area Network.

Watchers Specialized intelligence personnel who maintain surveillance on targeted individuals.

Watermarking The impression of a subtle pattern on paper using water. A watermark is only visible when the paper is held up to a light.

Watershed The area contributing water to a river, stream, lake, or ocean. Watersheds can be defined on several scales ranging from hundreds of square meters to millions of square kilometers.

Weapons of mass destruction Weapons that cause a high loss of life within a short time span. Nuclear, chemical, and biological weapons are classified as weapons of mass destruction.

Weapons-grade material Weapon-grade (or "bomb-grade") uranium or plutonium is any alloy or oxide compound that contains enough of certain isotopes of these elements to serve as the active ingredient in a nuclear weapon.

Whistle-blower A person inside an organization such as a corporation or government agency who comes forward with evidence of wrongdoing by the organization.

WHO World Health Organization.

Windtalkers The code name given to the Navajo Indian code talkers employed by United States military intelligence during World War II. Agents developed several encryption methods and code systems during the war, but a code based on the ancient Navajo language was one of the most successful codes ever used. It remained unbroken throughout the course of the war.

Wiretapping The act or instance of breaking into a telephone line to monitor a conversation or conversations. Wiretapping is usually illegal, though it may be applied by law-enforcement organizations with a search warrant.

WMD Weapons of mass destruction.

World Islamic Front for Jihad A group absorbed by Al-Qaeda (also known as Al-Qaida).

Yperite Mustard agent or gas.

Zoonoses Diseases transmitted from animals.

This page intentionally left blank

Chronology

c.6000 B.C. The rise of the great ancient civilizations, beginning 6,000 years ago in Mesopotamia, begat institutions and persons devoted to the security and preservation of their ruling regimes and founded the need for espionage, intelligence, and security operations.

c.3500 B.C. Underground passages first used as hiding places and escape routes during times of war.

c.1980 B.C. Egyptian pharaoh Amenemhet I is targeted as one of the first recorded victims of political assassination.

c.1500 B.C. Between 1500 B.C. and 1200 B.C., Greece's many wars with its regional rivals lead to the development of new military and intelligence strategies. The early Greeks relied on deception as a primary means of achieving surprise attacks on their enemies.

c.1000 B.C. From 1,000 B.C. onwards, Egyptian espionage operations focused on foreign intelligence about the political and military strength of rivals Greece and Rome. Egyptian spies were the first to develop the extensive use of poisons, including toxins derived from plants and snakes, to carry out assassinations or acts of sabotage.

c.500 B.C. Chinese military logician Sun-tzu stresses the importance of intelligence gathering and deception in his treatise *The Art of War.* In this work, added to by later philosophers, Sun-tzu detailed methods of espionage that included the use of defectors, double agents, and organized spy rings.

c.480 B.C. Demaratus of Sparta uses an early form of secret writing, concealing a message on a wooden tablet covered with wax to warn his countrymen of invasion by the Persian empire.

c.400 B.C. The Spartans use a cryptographic system called a *scytale* on papyrus wrapped around wooden scrolls.

c.400 B.C. Tunneling first used in warfare.

c.300 B.C. *Arthasastra*, an ancient Indian manual on politics, discusses mining, metallurgy, medicine, pyrotechnics, poisons, and fermented liquors.

c.300 B.C. During the Etruscan wars, Roman consul Fabius Maximus sends his brother to spy on Umbrians. Romans develop use of intelligence to gain treaties and scout military forces.

44 B.C. Assassination of Julius Caesar; records have established that the Roman intelligence community knew of the plot and even provided information to Caesar or his assistants providing the names of several conspirators. In a pattern to be repeated throughout the ages, the information from the intelligence community was ignored.

c.100 A.D. Roman records dating to the first century mention the presence of a secret police force, the *frumentarii*.

c.900 A.D. Lack of records conceals facts of espionage during the Middle Ages, but the birth of large nation-states, such as France and England, in the ninth and tenth centuries facilitated the need for intelligence in a diplomatic setting.

1095 Pope Urban II calls for the first Crusade, a military campaign to recapture Jerusalem and the Holy Lands from Muslim and Byzantine rule. Over the next four centuries, the Catholic Church masses several large armies, and employs spies to report on defenses surrounding Constantinople and Jerusalem. Special intelligence agents also infiltrate prisons to free captured crusaders, and sabotage rival palaces, mosques, and military defenses.

c.1200 Thirteenth-century Church councils establish laws regarding the prosecution of heretics and anti-clerical political leaders. The ensuing movement became known as the Inquisition. Espionage was an essential component of the Inquisition. The Church relied on vast networks of informants to find and denounce suspected heretics and political dissidents.

1245 A Franciscan monk, Carpini, is used by Pope Innocent IV to gather intelligence about Mongols.

1520 Niccolo Machiavelli, a Florentine political philosopher, publishes a series of book detailing the qualities and actions of effective rulers. In his works, *The Prince*, and *The Art of War*, Machiavelli advocates that rulers routinely employ espionage tradecraft,

engaging in deception and spying to insure protection of their power and interests. His advice, much of which was culled from rediscovered works of Aristotle and Cicero, was intended for the ruling Medici princes of Florence. However, the works gained popularity several centuries after their 1520 publication.

c.1550 Henry VIII and his daughter Elizabeth I nurture a spy network to locate and infiltrate Catholic loyalist cells that threaten the English monarchy. The Elizabethan intelligence community employs linguists, scholars, authors, engineers, and scientists, relying on professional experts to seek and analyze intelligence information.

1574 Francis Walsingham, joint secretary of state under Queen Elizabeth I of Britain, mounts an elaborate and effective spy network that uncovers a plot against Elizabeth by the imprisoned Mary, Queen of Scots, who was then executed. Later, in 1587, the spy network provides Elizabeth with information warning of the impending attack of the Spanish Armada.

1593 Christopher Marlowe, English dramatist/playwright/poet, is murdered in a Deptford tavern after being accused of being a spy.

c.1600 Chemists invent invisible inks, and the rebirth of complex mathematics revives long-dormant encryption and code methods. Later, in the Scientific Revolution and the Enlightenment, the development of telescopes, magnifying glasses, the camera obscura, and clocks facilitates remote surveillance and the effective use of "dead drops" to pass information between agents.

1670 Secret treaty between Charles II and Louis XIV.

c.1700 The Age of Empires: espionage further develops in the numerous conflicts and wars that occur in Europe and between rival colonial powers in Europe and abroad. Industrialization, economic and territorial expansion, the diversification of political philosophies and regimes, and immigration all transform the world's intelligence communities.

1703 Although concepts of disease are primitive, in an act of biological warfare, Sir Jeffrey Amherst, commander-in-chief of British forces in North America, suggests grinding the scabs of smallpox pustules into blankets intended for Native American tribes known to trade with the French.

1776 Benjamin Thompson (Count Rumford), an English physicist whose work contributed to the formulation of the second law of thermodynamics, acts as Tory spy during the American Revolution.

1776 Nathan Hale hanged by the British as a spy during the American Revolution. His last words are reputed to have been, "I only regret that I have but one life to give for my country."

1780 General Benedict Arnold betrays the colonial revolution when he promises secretly to surrender the fort at West Point to the British army. Arnold flees to England; his co-conspirator, British spy Major John Andre, is hanged.

1789 Congress passes the Judiciary Act, which establishes the federal justice system and creates the Office of the Attorney General, as well as the U.S. Marshal Service.

1789 U.S. Customs Service begins operation on July 31.

1789 Congress establishes the Department of State on September 15.

1789 French spy Richeborg (a dwarf) is disguised as a baby in diapers, and carried in girl's arms, so he can eavesdrop on conversations and carry secret letters through Paris during the French Revolution.

1789 During the French Revolution, Robespierre's informant networks denounce traitors to the new republic and track down refugee aristocrats and clergy for trial and execution. The wide application of treason charges marks one of the greatest abuses of intelligence powers in the modern era.

1790 France introduces the metric system.

1794 First army air corps established when revolutionary France creates a military balloon contingent.

1795 Martin Heinrich Klaproth, German chemist, isolates a new metal and names it titanium, after the Titans of Greek mythology. He gives full credit to English mineralogist William Gregor, who first discovered it in 1791.

1798 Government legislation is passed to establish hospitals in the United States devoted to the care of ill mariners. This initiative leads to the establishment of a hygenic laboratory, which eventually grows to become the National Institutes of Health.

1798 Geologists accompany Napoleon's expeditionary force to Egypt.

1798 U.S. Congress establishes the Department of the Navy, which also includes the Marine Corps.

1799 Chinese emperor Kia King's ban on opium fails to stop the lucrative British opium trade.

1800 Records indicate use of chloral hydrate in the "Mickey Finn," an anesthetic cocktail used to abduct or lure sailors to serve on ships bound for sea.

1800 Alessandro Giuseppe Antonio Anastasio Volta, Italian physicist, announces his invention of the voltaic pile, which is the first battery. His work duplicating Galvani's 1791 "animal electricity" experiment leads him to discover that it is the contact of dissimilar metals that causes the electricity. He arranges suitable pairs of metallic plates in a certain order, separates them by pieces of leather soaked in brine, and creates a pile, or battery, that produces a continuous and controllable electric current.

c.1800 Colonial rulers and powers employ secret police and agents of espionage throughout their territorial holdings, hoping to quell anti-colonial rebellions and separatist movements.

1802 John Dalton introduces modern atomic theory into the science of chemistry.

1804 Joseph Fouché, a French revolutionary and minister of police, sets up the first modern police state, and uses his spy network to uncover and foil a plot by George Cadoudal against Napoleon Bonaparte.

1805 Joseph-Louis Gay-Lussac, French chemist, establishes that precisely two volumes of hydrogen combine with one volume of oxygen to form water.

1812 Second U.S. war with Great Britain, commonly called the War of 1812.

1817 German pharmacist Frederick Serturner announces the extraction of morphine from opium.

1818 Augustin-Jean Fresnel, French physicist, publishes his *Mémoire sur la diffraction de la lumière* in which he demonstrates the ability of a transverse wave theory of light to account for such phenomena as reflection, refraction, polarization, interference, and diffraction patterns.

1820 André Marie Ampère, French mathematician and physicist, extends Ørsted's work and formulates one of the basic laws of electromagnetism.

1823 Monroe Doctrine declares Western Hemisphere a U.S. "sphere of influence."

1827 Georg Simon Ohm, German physicist, experiments with electricity using wires of different length and diameter and discovers that a long, thick wire passes less current than a short, thin wire. He states what becomes Ohm's law.

1828 Friedrich Wöhler synthesizes urea. This is generally regarded as the first organic chemical produced in the laboratory, and an important step in disproving the idea that only living organisms can produce organic compounds. Work by Wöhler and others establish the foundations of organic chemistry and biochemistry.

1828 Luigi Rolando, Italian anatomist, achieves the first synthetic electrical stimulation of the brain.

1831 Michael Faraday, English physicist and chemist, discovers electromagnetic induction. After laboring for ten years to achieve the opposite of what Ørsted had done—to convert magnetism into electricity—he finally produces for the first time an induction current using a magnet. This is the first electric generator. With such a device, mechanical energy can be converted into electrical energy.

1837 Invention of the Daguerreotype, the first practical form of photography. When widely incorporated into intelligence practices in the 1860s, the photograph permitted agents of espionage to portray targets, documents, and other interests.

1839 First Opium War begins between Britain and China. The conflict lasts until 1842. Imperial Chinese commissioner Lin Tse-hsü seizes or destroys vast amounts of opium, including stocks owned by British traders. The result was a Chinese payment of an indemnity of more than 21 million silver dollars and Hong Kong being ceded to Britain under the Treaty of Nanking.

1839 Theodore Schwann extends the theory of cells to include animals and helps establish the basic unity of the two great kingdoms of life. He publishes *Microscopical Researches into the Accordance in the Structure and Growth of Animals and Plants*, in which he asserts that all living things are made up of cells, and that each cell contains certain essential components. He also coins the term "metabolism" to describe the overall chemical changes that take place in living tissues.

1839 Invention of microfilm by John Dancer.

1840 Friedrich Gustav Jacob Henle publishes the first histology textbook, *General Anatomy*. This work includes the first modern discussion of the germ theory of communicable diseases.

1841 Eugene-Melchoir Peligot isolates the element uranium.

1843 Charles-Frédéric Gerhardt, French chemist, simplifies chemical formula-writing, so that water becomes H_20 instead of the previous H_40_2.

1843 Howard Aiken develops first mechanical programmable calculator.

1844 Samuel Morse sends the first message via telegraph. His code (Morse code) and telegraph were able to send messages over lines in a matter of minutes, requiring only knowledge of the operational code. As soon as governments began to use telegraphs to send vital communications, rival intelligence services learned to tap the line, gaining access to secret communications and conducting detailed surveillance from a comfortable distance. Use of the telegraph necessitated the development of complex codes and the creation of specialized cryptology departments. By the turn of the twentieth century, most national intelligence operations in Europe and the United States were involved communications surveillance and the tapping of both wired and wireless telegraphs.

1845 Christian Friedrich Schönbein, German-Swiss chemist, prepares guncotton. He discovers that a certain acid mixture combines with the cellulose in cotton to produce an explosive that burns without smoke or residue.

1846 Ascanio Sobrero, Italian chemist, slowly adds glycerin to a mixture of nitric and sulfuric acids and first produces nitroglycerine. He is so impressed by the explosive potential of a single drop in a heated test tube and so fearful of its use in war that he makes no attempt to exploit it. It is another 20 years before Alfred Nobel learns the proper formula and puts it to use.

1846 U.S. forces victorious in Mexican War, which results in annexation of what is today the southwestern United States.

1848 U.S. Congress passes Drug Importation Act that allows U.S. Customs Service inspection to stop entry of foreign drugs.

1849 First aerial bombardment campaign, by Austrians against Venetians, using 200 unpiloted hot-air balloons containing bombs set on timers.

1852 Jean Foucault invents gyroscope, an important instrument still used in modern navigation and guidance systems.

1855 Henri-Etienne Sainte-Claire Deville, French chemist, first produces aluminum in a pure state. He produces the metal in quantity by heating aluminum chloride with metallic sodium.

1856 Second Opium War begins between Britain and China. The conflict lasts until 1860. Also known as the Arrow War, or the Anglo-French War in China, the war broke out after a British-flagged ship, the *Arrow*, is impounded by China. France joins Britain in the war after the murder of a French missionary. China is again defeated, resulting in another large indemnity and the legalization of opium under the Treaty of Tientsin.

1857 Louis Pasteur demonstrates that lactic acid fermentation is caused by a living organism. Between 1857 and 1880, he performs a series of experiments that refute the doctrine of spontaneous generation. He also introduces vaccines for fowl cholera, anthrax, and rabies, based on attenuated strains of viruses and bacteria.

1858 Charles Darwin and Alfred Russell Wallace agree to a joint presentation of their theory of evolution by natural selection.

1858 Rudolf Ludwig Carl Virchow publishes his landmark paper "Cellular Pathology" and establishes the field of cellular pathology. Virchow asserts that all cells arise from preexisting cells (*Omnis cellula e cellula*). He argues that the cell is the ultimate locus of all disease.

1858 A group of the Irish Republican Brotherhood (IRB) forms another revolutionary group, the Fenian Brotherhood, with the goal of freeing Ireland from British rule.

1861 U.S. Civil War (1861–1865). Morphine gains wide medical use during the conflict.

1861 President-elect Abraham Lincoln arrives secretly in Washington to foil assassination plot brewing in Baltimore.

1861 Balloonist and Ohioan Thaddeus Lowe is accused by irate South Carolina citizens of being a Yankee spy after his balloon lands following a 500 mile aerial flight. Lowe eventually volunteers his services to Union forces and becomes director of the Union's balloon corps. His resignation two years later brings the corps to an end.

1861 Rose O'Neal Greenhow is arrested as Confederate spy after warning General P.G.T. Beauregard of a planned Union attack on Manassas in July 1861. She is released in 1862 but dies in a shipwreck.

1862 Department of Agriculture establishes the Bureau of Chemistry, the organizational forerunner of the Food and Drug Administration.

1862 Legal Tender Act authorizes the U.S. government to issue currency notes through the Treasury Department. These notes, which Treasury continues to issue until 1971, are known as U.S. notes.

1862 In September, President Lincoln suspends the right of *habeas corpus* in order to allow federal authorities to arrest and detain suspected Confederate sympathizers and draft resisters without arrest warrants or speedy trials. The following year, Congress reaffirms the suspension in the *Habeas Corpus* Act of 1863.

1863 Ferdinand Reich, German mineralogist, and his assistant Hieronymus Theodor Richter examine zinc ore spectroscopically and discover the new, indigo-colored element iridium. It is used in the next century in the making of transistors.

1863 Geology plays decisive role in the Battle of Gettysburg as Union troops hold key high-ground positions.

1863 Belle Boyd, a Confederate spy, is released from prison in Washington.

1864 James Clerk Maxwell develops equations of electromagnetic wave propagation.

1864 First Geneva Convention addresses "the amelioration of the condition of the wounded on the field of battle," resulting in principles for protecting noncombatant personnel caring for the wounded. The convention also establishes the International Red Cross.

1865 An epidemic of rinderpest kills 500,000 cattle in Great Britain. Government inquiries into the outbreak pave the way for the development of contemporary theories of epidemiology and the germ theory of disease.

1865 Gregor Mendel presents his work on hybridization of peas to the Natural History Society of Brno, Moravia. The paper is published in the 1866 issue of the society's *Proceedings*. Mendel presents statistical evidence that hereditary factors are inherited from both parents in a series of papers on "Experiments on Plant Hybridization" published between 1866 and 1869. His experiments provide evidence of dominance, the laws of segregation, and independent assortment, although the work is generally ignored until 1900.

1865 U.S. Secret Service established to interdict counterfeit currency and its manufacturers.

1865 President Lincoln is shot in Washington, D.C., by John Wilkes Booth. Lincoln dies the next day; Andrew Johnson assumes the presidency.

1865 The Molly McGuires, a secret society of Irish miners, attacks coal-mine operators and owners for mistreatment of workers.

1867 Alfred Nobel, Swedish inventor, invents dynamite, a safer and more controllable version of nitroglycerine. He combines nitroglycerine with "kieselguhr," or earth containing silica, and discovers that it cannot be exploded without a detonating cap.

1867 Secret Service responsibilities broadened to include "detecting persons perpetrating frauds against the government."

1869 Dimitri Ivanovich Mendeleev, Russian chemist, and Julius Lothar Meyer, German chemist, independently put forth the Periodic Table of Elements, which arranges the elements in order of atomic weights. However, Meyer does not publish until 1870, nor does he predict the existence of undiscovered elements as Mendeleev does.

1870 Lambert Adolphe Jacques Quetelet showes the importance of statistical analysis for biologists and provides the foundations of biometry.

1870 Congress creates the Department of Justice.

1871 U.S. president Ulysses S. Grant establishes Office of the Surgeon General.

1872 Ferdinand Julius Cohn publishes the first of four papers entitled "Research on Bacteria," which establishes the foundation of bacteriology as a distinct field. He systematically divides bacteria into genera and species.

1873 James Clerk Maxwell, Scottish mathematician and physicist, publishes *Treatise on Electricity and Magnetism* in which he identifies light as an electromagnetic phenomenon. He determines this when he finds his mathematical calculations for the transmission speed of both electromagnetic and electrostatic waves are the same as the known speed of light. This landmark work brings together the three main fields of physics—electricity, magnetism, and light.

1876 German bacteriologist Robert Koch publishes a paper on anthrax that implicates a bacterium as the cause of the disease, validating the germ theory of disease.

1876 Alexander Graham Bell patents the telephone.

1876 The first microphone is invented by Emile Berliner.

1877 Congress passes legislation prohibiting the counterfeiting of any coin, gold, or silver bar.

1878 Charles–Emanuel Sedillot introduces the term "microbe." The term becomes widely used as a term for a pathogenic bacterium.

1878 In a backlash against 12 years of martial law in the southern United States, Congress passes the Posse Comitatus Act, which forbids the military from enforcing domestic law.

1880 First attempt at passage of a nationwide food and drug law. Although defeated in Congress, U.S. Department of Agriculture's findings of widespread food adulteration spur continued interest in food and drug legislation.

1880 Louis Pasteur develops a method of weakening a microbial pathogen of chicken, and uses the term "attenuated" to describe the weakened microbe.

1881 President James A. Garfield is shot on July 2, 1881, in Washington, D.C., by anarchist Charles J. Guiteau. Garfield dies on September 19; Chester A. Arthur assumes the presidency.

1882 Robert Koch discovers the tubercle bacillus and enunciates "Koch's postulates," which define the classic method of preserving, documenting, and studying bacteria.

1882 Establishment of the Office of Naval Intelligence, which by the early twenty-first century will be the oldest continually operating intelligence agency in the United States.

1883 George Francis Fitzgerald, Irish physicist, first suggests a method of producing radio waves. From his studies of radiation, he concludes that an oscillating current will produce electromagnetic waves. This is later verified experimentally by Hertz in 1888 and used in the development of wireless telegraphy.

1883 U.S. Secret Service is officially embodied as a distinct organization within the Treasury Department.

1883 British inventor Hiram Stevens Maxim invents the machine gun.

1884 Louis Pasteur and coworkers publish a paper titled "A New Communication on Rabies." Pasteur proves that the causal agent of rabies can be attenuated and the weakened virus can be used as a vaccine to prevent the disease. This work serves as the basis of future work on virus attenuation, vaccine development, and the concept that variation is an inherent characteristic of viruses.

1885 U.S. Army establishes its Division of Military Information, its formal military intelligence organization.

1887 Ernst Mach, Austrian physicist, is the first to note the sudden change in the nature of the airflow over a moving object that occurs as it approaches the speed of sound. Because of this, the speed of sound in air is called Mach 1. Mach 2 is twice that speed, and so on.

1888 Heinrich Rudolf Hertz, German physicist, for the first time generates electromagnetic (radio) waves and devises a detector that can measure their wavelength. From this he is able to prove experimentally James Clerk Maxwell's hypothesis that light is an electromagnetic phenomenon. Hertz's work not only discovers radio waves, but experimentally unites the three main fields of physics—electricity, magnetism, and light.

1889 Frederick Augustus Abel, English chemist, and James Dewar, Scottish chemist and physicist, invent cordite and pioneer the production of smokeless powder. Their new mixture borrows from previous discoveries but proves safer to handle.

1889 Johann Philipp Ludwig Julius Elster and Hans Friedrich Geitel, both German physicists, study the photoelectric effect (when an electric current is created upon the exposure of certain metals to light) and produce the first practical photoelectric cells that can measure the intensity of light.

1890 Oliver Joseph Lodge, English physicist, invents the coherer, a detector of radio waves that, although replaced, makes him one of the pioneers of early radio communication. He also suggests correctly that the sun emits radio waves.

1892 George M. Sternberg publishes his *Practical Results of Bacteriological Researches*. Sternberg's realization that a specific antibody was produced after infection with vaccinia virus and that immune serum could neutralize the virus becomes the basis of virus serology. The neutralization test provides a technique for diagnosing viral infections, measuring the immune response, distinguishing antigenic similarities and differences among viruses, and conducting retrospective epidemiological surveys.

1892 U.S. Congress awards Harriet Tubman a pension for her work as a Union nurse, spy and scout during the Civil War.

1894 U.S. Secret Service begins part-time protection of U.S. president Grover Cleveland.

1895 Wilhelm Conrad Röntgen, German physicist, discovers x rays. While working on cathode ray tubes and experimenting with luminescence, he notices that a

nearby sheet of paper that is coated with a luminescent substance glows whenever the tube is turned on. For seven weeks he continues to experiment, and near the end of the year is able to report the basic properties of the unknown rays he names "x rays."

1896 Antoine-Henri Becquerel, French physicist, discovers radioactivity in uranium ore.

1896 Guglielmo Marconi, Italian electrical engineer, travels to England to apply for and obtain the first patent in the history of radio. By this time, he has sent and received a radio signal over nine miles.

1896 Johann Elster and Hans Friedrich Geitel study the newly discovered radioactivity and demonstrate that external effects do not influence the intensity of radiation. They are also the first to characterize radioactivity as being caused by changes that occur within the atom.

1897 Joseph John Thomson, English physicist, discovers the electron. He conducts cathode ray experiments and concludes that the rays consist of negatively charged "electrons" that are smaller in mass than atoms.

1898 Marie Sklodowska Curie and Pierre Curie discover the radioactive element radium. They spend the next four years refining eight tons of pitchblende to obtain a full gram of radium.

1898 Spanish-American War.

1899 First Hague Conference establishes international laws of conduct in warfare.

1900 Carl Correns, Hugo de Vries, and Erich von Tschermak independently rediscover Mendel's laws of inheritance. Their publications mark the beginning of modern genetics. Using several plant species, de Vries and Correns perform breeding experiments that parallel Mendel's earlier studies and independently arrive at similar interpretations of their results. Therefore, upon reading Mendel's publication, they immediately recognized its significance. William Bateson describes the importance of Mendel's contribution in an address to the Royal Society of London.

1900 Ernest Rutherford, British physicist, first determines radioactive half-life.

1900 Friedrich Ernst Dorn, German physicist, demonstrates that radium emits a gas as it produces radioactivity. This proves to be the first evidence that in the radioactive process one element is actually transmuted into another.

1900 Karl Landsteiner discovers the blood-agglutination phenomenon and the four major blood types in humans.

1901 President William McKinley is assassinated by anarchist Leon Czolgosz.

1901 United States acquires rights from Cuba to use Guantanamo Bay indefinitely as a naval base.

1901 Antoine Henri Becquerel, French physicist, studies the rays emitted by the natural substance uranium and concludes that the only place they could be coming from is within the atoms of uranium. This marks the first clear understanding of the atom as something more than a featureless sphere. Becquerel's discovery of radioactivity and his focus on the uranium atom make him the father of modern atomic and nuclear physics.

1901 After the assassination of President William McKinley, Congress formally places the U.S. Secret Service—which first began guarding presidents during the second Grover Cleveland administration seven years before—in charge of protecting the president.

1901 Henry Classification System devised for fingerprint analysis by Sir Edward Henry.

1902 The Secret Service assumes full-time responsibility for protection of the president. Two operatives are assigned full time to the White House detail.

1902 U.S. Congress passes Spooner Act, which authorizes the United States to purchase the assets of a French company that had attempted to build a canal through Panama, and to begin a U.S. effort toward building a canal.

1902 Oliver Heaviside, English physicist and electrical engineer, and Arthur Edwin Kennelly, British-American electrical engineer, independently and almost simultaneously make the first prediction of the existence of the ionosphere, an electrically conductive layer in the upper atmosphere that reflects radio waves. They theorize correctly that wireless telegraphy works over long distances because a conducting layer of atmosphere exists that allows radio waves to follow Earth's curvature instead of traveling off into space.

1903 For their work in the physics of radioactivity, Antoine Becquerel, Pierre Curie, and Marie Curie are awarded the Nobel Prize for physics.

1903 Panama secedes from Colombia. The new government will cooperate in the building of the Panama Canal.

1903 U.S. Army implements the concept of a permanent general staff, and with it the idea, pioneered in Europe, of the four sections of a military command. The Division of Military Information thus becomes G-2.E170.

1903 Orville and Wilbur Wright make the first powered flight.

1904 Roosevelt Corollary to the Monroe Doctrine asserts that the United States has the right to assume the defacto role of an international police power.

1904 Congress creates Panama Canal Zone, and in the summer construction on the Panama Canal begins.

1905 Bloody Sunday incident in Russia. Tsarist troops fire on marchers in St. Petersburg.

1905 Sinn Fein political movement for Irish independence is founded.

1905 Albert Einstein, German-Swiss physicist, publishes his second paper on relativity including his famous equation stating the relationship between mass and energy: $E = mc^2$. In this equation, E is energy, m is

mass, and c is the velocity of light. This contains the revolutionary concept that mass and energy are simply different aspects of the same phenomenon.

1906 Congress passes Sundry Civil Expenses Act, which provides funds for presidential protection by the Secret Service.

1906 Secret Service operatives began to investigate the western land frauds. The investigations return millions of acres of land to the government. Operative Joseph A. Walker is murdered on November 3, 1907, while working on one of these cases, becoming the first operative killed in the line of duty.

1907 Triple Entente formed as Great Britain formally joins the defense pact between France and Russia.

1907 Bertram Borden Boltwood, American chemist and physicist, discovers what he believes is a new element which he calls ionium. It is later determined to be a radioactive isotope of thorium. Boltwood also invents a radioactive dating procedure.

1907 Second Hague Conference establishes further international laws of conduct in warfare, with a focus on war in a maritime environment.

1907 Establishment of Aeronautical Section of the U.S. Army Signal Corps—first incarnation of the U.S. Air Force. This becomes the Aviation Section in 1914.

1908 Large deposits of petroleum are discovered in the Middle East.

1908 Ernest Rutherford and Hans Wilhelm Geiger develop an electrical alpha-particle counter. Over the next few years, Geiger continues to improve this device which becomes known as the Geiger counter.

1908 Secret Service begins protecting the president-elect.

1908 A Sundry Civil Service Bill declares that Secret Service employees accepting assignments by any department other than Treasury (except in counterfeiting cases) would be suspended for two years. The provision became effective July 1, and prevented the practice of agencies like the Department of Justice (DOJ) borrowing investigators for specific cases.

1908 Formal beginning of the Bureau of Investigation (BOI), which became the FBI in 1935.

1909 U.S. Congress passes Copyright Law.

1909 Alfred Stock, German chemist, first synthesizes boron hydrides (compounds of boron and hydrogen). Forty year later, boron hydrides prove useful to space exploration as additives to rocket fuel.

1909 An intelligence report in the British Parliament leads to the establishment of the Secret Service Bureau, precursor to both MI5 and MI6.

1910 The United States sends military forces to Mexico during Mexican revolution.

1910 Britain signs an agreement with China to dismantle the opium trade. However, the profits made from its cultivation, manufacture, and sale were so enormous that no serious interruption would be effected until World War II closed supply routes throughout Asia.

1910 Congress passes the White Slave Traffic Act on June 25. Also known as the Mann Act, this new law significantly increases BOI jurisdiction over interstate crime.

1911 At 11:01 a.m. on January 18, the U.S. Navy's Eugene Ely lands a Curtiss pusher aircraft on a specially built platform aboard the USS *Pennsylvania.* Thus is born the concept of the aircraft carrier.

1911 Fritz Pregl, Austrian chemist, first introduces organic microanalysis. He invents analytic methods that make it possible to determine the empirical formula of an organic compound from just a few milligrams of the substance.

1911 Heike Kamerlingh-Onnes, Dutch physicist, first discovers the phenomenon of superconductivity when he studies the properties of certain metals subjected to the low temperatures of liquid helium. He finds that some metals, like mercury and lead, undergo a total loss of electrical resistance. He also discovers that a form of liquid helium is produced which has properties unlike any other substances.

1911 Marie Curie receives the Nobel Prize in chemistry for the discovery of the elements radium and polonium, for the isolation of radium, and for investigating its compounds. It is Curie's second Nobel Prize.

1911 Georg von Hevesy conceives the idea of using radioactive tracers. Von Hevesy later wins the Nobel Prize in 1943.

1911 Italians make first use of aircraft in combat during 1911–12 war against Turkey. On October 23, Italians conduct first reconnaissance in an airplane, against Turkish troops near Tripoli in what is now Libya. On November 1, the Italians again make aviation history when they conduct the first aerial bombing raid against an enemy.

1912 U.S. Marines invade Honduras, Cuba, and Nicaragua to protect American interests. U.S. troops will remain in Nicaragua until 1930s.

1912 The U.S. Public Health Service is established.

1912 Joseph Thomson develops a forerunner of mass spectrometry and separation of isotopes.

1912 Max von Laue, German physicist, obtains diffraction pattern for x rays through a crystal and offers evidence that x rays are a form of electromagnetic radiation and are waves. This marks the beginning of studies on the physics of solids as an analysis of the periodic and regular disposition of atoms in a crystal.

1912 Paul Ehrlich discovers a chemical cure for syphilis. This is the first chemotherapeutic agent for a bacterial disease.

1912 Theodore Roosevelt survives assassination attempt on October 14 in Milwaukee while campaigning for a second term as president.

1913 U.S. troops assist in pursuit of Mexican rebel leader Francisco Pancho Villa in northern Mexico.

1913 Congress authorizes permanent protection of the president and the statutory authorization for president-elect protection.

1913 Harry Brearly, English metallurgist, accidentally discovers a nickel-chromium alloy that is corrosion resistant. It becomes stainless steel.

1913 Max Bodenstein, German physical chemist, develops the concept of a chain reaction in which one molecular change triggers another, and so on.

1913 U.S. Congress passes Federal Reserve Act, creating Federal Reserve System.

1913 Ratification of Sixteenth Amendment to the Constitution, which gives Congress power to levy taxes.

1914 The assassination of Austrian Archduke Francis Ferdinand precipitates World War I.

1914 World War I places additional responsibilities on the BOI. On April 6, 1917, Congress declares war on Germany and President Woodrow Wilson authorizes the BOI to detain enemy aliens.

1914 Panama Canal opens on August 15.

1915 Germany uses poison gas at the Battle of Ypres.

1915 A U-boat sinks the British ship *Lusitania,* a passenger ship also carrying military supplies from the United States to Britain.

1915 Frederick William Twort publishes the landmark paper *An Investigation of the Nature of Ultra-Microscopic Viruses*. Twort notes the degeneration of bacterial colonies and suggests that the causative agent is an ultra-microscopic-filterable virus that multiplies true to type.

1915 President Wilson directs the secretary of the treasury to have the Secret Service investigate espionage in the United States.

1915 U.S. Coast Guard founded.

1915 British nurse Edith Cavell is shot as a spy by a German firing squad for assisting British soldiers seeking to escape the Germans.

1915 After denouncing them as spies, the United States expels German attaches.

1916 German use of zeppelins, important both as surveillance craft and bombers during the first two years of World War I, begins to decline in September, after Allies develop special explosive bullets capable of downing airships.

1916 The Black Tom explosion. On July 29, German agents set fire to a complex of warehouses and ships in the New York harbor that hold munitions, fuel, and explosives bound to aid the Allies in their fight. Though the United States is technically a neutral nation at the time of the attack, their general policies greatly favor the Allies. The attack persuades many that the United States should join the Allies and intervene in the war in Europe.

1916 The Home Section of the British Secret Service Bureau becomes MI5, or the Security Service.

1916 Mexican guerrilla leader Pancho Villa conducts a raid on Columbus, New Mexico, killing 17 Americans.

1917 The British issue a declaration calling for a Jewish homeland in Palestine.

1917 Congress authorizes permanent protection of the president's immediate family and "threats" directed toward the president become a federal violation.

1917 Tsarist Russia's February Revolution begins with rioting and strikes in St. Petersburg. Alexander Kerensky ultimately assumes control of democratic socialist provisional government, exposes undercover agents of the Okhrana.

1917 British signal intelligence, having cracked the German cipher, intercepts a message from German foreign minister Arthur Zimmermann to the Mexican president, promising to return territories Mexico had lost to the United States in the Mexican War if Mexico will enter the war on Germany's side.

1917 Mata Hari (the pseudonym of Dutch dancer Margaretha Geertruida Zelle), who joined the German secret service in 1907, is executed by French firing squad. Mata Hari betrayed many military secrets that were gained from Allied officers who were on intimate terms with her.

1917 United States declares war on Germany.

1917 The U.S. Army creates the Cipher Bureau within the Military Intelligence Division.

1917 American engineer Gilbert S. Vernam develops the first significant automated encryption and decryption device when he brings together an electromagnetic ciphering machine with a teletypewriter.

1917 U.S. Congress passes the Espionage Act, criminalizing the disclosure of military, industrial, or government secrets related to national security. The act also prohibits antiwar activism and refusal of conscription, sparking controversy.

1917 V.I. Lenin returns from exile to Russia following Romanov abdication of the Russian throne. Lenin leads a Bolshevik revolution in November.

1918 German radio officer Fritz Nebel develops the ADFGX cipher.

1918 Russia signs the Brest-Litovsk treaty, ending Russian participation in World War I.

1918 Bolsheviks execute Tsar Nicholas II and his family.

1918 Major Joseph O. Mauborgne of the U.S. Army devises the one-time pad, whereby sender and receiver possess identical pads of cipher sheets that are used once and then destroyed—a virtually unbreakable system.

1918 German engineer Arthur Scherbius invents a three-rotor cipher machine, the Enigma.

1918 Germany's Kaiser Wilhelm II abdicates and World War I ends in Europe after 20 million casualties and six million deaths.

1918 U.S. president Wilson's fourteen-point peace proposal introduced.

1918 Sedition Act of 1918 amends Espionage and Sedition Acts to broaden the arrest powers granted to federal agents in apprehending and detaining individuals suspected of treason or antiwar activity.

1918 Socialist Party leader Eugene V. Debs is convicted and sentenced to a ten-year prison term under the Espionage Act for an antiwar speech he delivers in Canton, Ohio. Debs is later pardoned by President Warren G. Harding in December 1921.

1918 Hungary overthrows the Austro-Hungarian monarchy.

1918 An influenza epidemic spreads across Asia and war-ravaged Europe to the Americas. The epidemic eventually kills 20 million people, including 500,000 Americans.

1919 The Treaty of Versailles requires Germany, now under the Weimar Republic, to cede territory to France, Belgium, and Poland; relinquish its colonies; and pay extensive war reparations that will eventually cripple the German economy. The U.S. Senate refuses to ratify the treaty.

1919 U.S. House of Representatives refuses to seat socialist Victor Berger, a congressman elected from Wisconsin.

1919 U.S. fears increase after anarchist groups target government and business leaders with bombs in April and May; the terrorist wave culminates in a series of bombings in eight U.S. cities on June 2. Under the orders of Attorney General A. Mitchell Palmer, federal agents begin round-up of suspected communists and anarchists in November. The Palmer Raids, as they became known, last until March 1920 and result in the arrest of 6,000 suspects.

1919 Anarchists Emma Goldman and Alexander Berkman are deported by the United States to Russia.

1919 Establishment of British Government Code and Cypher School (GC&CS) in November.

1919 Congress passes the National Motor Vehicle Theft Act, also known as the Dyer Act, on October 28. This act authorizes the Bureau of Investigation to investigate auto thefts that cross state lines.

1920 The League of Nations first meets in Geneva.

1920 Bolshevist or anarchist terrorists accused of September 16 bombing on Wall St. in New York City which kills 35 people and injures hundreds more.

1920 Iraq is placed under British mandate.

1921 Except for six counties in Protestant Northern Ireland, the British Parliament grants Ireland dominion status.

1921 William Marston develops first modern polygraph.

1921 Twenty-six-year-old J. Edgar Hoover is named assistant director of BOI.

1922 Militants in the Irish Sinn Fein party form the Irish Republican Army (IRA).

1922 White House police force created at request of President Warren G. Harding. Ultimately this will become the uniformed division of the U.S. Secret Service.

1922 On March 20, U.S. Navy commissions the *Langley,* its first aircraft carrier. Later that year, the United States and other powers sign the Washington Naval Limitation Treaty, which controls battleship inventories, thus spurring carrier production. Congress authorizes the conversion of the unfinished battleships *Lexington* and *Saratoga* to become the navy's second and third carriers.

1922 Benito Mussolini becomes Italian dictator and forms a Fascist government.

1923 Union of Soviet Socialist Republics (U.S.S.R.) formed.

1923 Adolf Hitler, leader of the German Nazi party, attempts to seize power. He is arrested and sentenced to prison.

1923 Works published before 1923 are now in the public domain, meaning that they no longer hold a copyright, though a particular translation, made more recently, may be copyrighted. For works published after 1923, there are specific provisions as to when the item becomes part of the public domain. Some of these provisions, and other aspects of U.S. copyright law, are governed by the Berne Convention for the Protection of Literary and Artistic Works, which the United States signed in 1989.

1924 Lenin dies, to be succeeded by a triumvirate of leaders headed by Joseph Stalin.

1924 The U.S. Navy creates its first cryptanalytic group within the Code and Signal Section of the Office of Naval Communications.

1924 From prison, Adolf Hitler publishes *Mein Kampf,* in which he outlines the plan for the conquest of eastern Europe and the extermination of the Jews, which he will undertake as German leader less than a decade later.

1924 J. Edgar Hoover designated director of the BOI.

1924 BOI establishes an identification division after Congress authorizes "the exchange of identification records with officers of the cities, counties, and states."

1925 France begins construction of defensive Maginot Line against future German aggression. The line eventually proves useless as Hitler's troops bypass the line during their 1940 conquest of France.

1925 Johannes Hans Berger, German neurologist, records the first human electroencephalogram (EEG).

1925 Patrick Blackett, English physicist, takes the first photographs of a nuclear reaction in progress. To achieve this he uses a Wilson cloud chamber and takes over 20,000 photographs of more than 400,000 alpha particle tracks and observes eight actual collisions of an alpha particle and a nitrogen molecule.

1925 Special Agent Edwin C. Shanahan becomes the first BOI agent killed in the line of duty.

1926 Jiang Jie-shi (Chiang Kai-shek) assumes control of the Chinese government.

1926 The passage of the Air Commerce Act creates the earliest predecessor of the FAA, called the Aeronautics Branch.

1926 U.S. Army Air Service becomes Army Air Corps.

1926 Emperor Showa Tenno Hirohito assumes power in Japan.

1926 U.S. forces intervene in Nicaragua against leftist nationalist insurgency led by Augusto Cesar Sandino.

1927 Jiang Jie-shi defeats Communist Mao Zedong's (Mao Tse-tung) ''Autumn Harvest" rebellion.

1927 Charles Lindbergh makes first nonstop solo transatlantic flight.

1927 German physicist Werner Heisenberg publishes uncertainty principle.

1928 George Gamow, Russian-American physicist, develops the quantum theory of radioactivity which is the first theory to successfully explain the behavior of radioactive elements, some of which decay in seconds and others after thousands of years.

1928 Hermann Weyl, German mathematician, publishes his *Gruppen theorie und Quatenmechanik* in which he shows that most of the regularities of quantum phenomena on the atomic level can be most simply understood using group theory. His book helps mold modern quantum theory.

1928 Sixty-two nations sign the Kellogg-Briand Pact (including the United States, Great Britain, Japan, and Italy) and renounce war as a means to solve international disputes.

1929 Kingdom of Serbs, Croats, and Slovenes becomes Yugoslavia.

1929 Scottish biochemist Alexander Fleming discovers penicillin. He observes that the mold *Penicillium notatum* inhibits the growth of some bacteria. This is the first antibiotic, and it opens a new era of "wonder drugs" to combat infection and disease.

1929 John Douglas Cockcroft, English physicist, and Irish physicist Ernest Thomas Sinton Walton devise the first particle accelerator, which produces proton beam energies up to 600,000 volts. Three years later, they will use the accelerator to bombard lithium and produce two alpha particles (having combined lithium and hydrogen to produce helium). This is the first nuclear reaction that has been brought about through the use of artificially accelerated particles and without the use of any form of natural radioactivity; it will prove highly significant to the creation of an atomic bomb.

1929 Julius Arthur Nieuwland, Belgian-American chemist, develops neoprene, the first successful synthetic rubber.

1929 U.S. stock market crash in October ushers in Great Depression.

1930 U.S. Food, Drug, and Insecticide Administration is renamed Food and Drug Administration (FDA).

1930 Nils Edlefsen constructs the first cyclotron under the direction of the American physicist Ernest Orlando Lawrence. This first instrument is a small machine that is used to produce directed beams of charged particles. Over the next few years, Lawrence continues to build larger instruments, which eventually contribute to the discovery of new elements.

1930 U.S. Treasury Department creates Bureau of Narcotics, which will remain the principal anti-drug agency of the federal government until the late 1960s.

1930 Establishment of U.S. Army Signal Intelligence Service (SIS) to consolidate all military operations in cryptography and cryptanalysis.

1930 Primitive anthrax vaccine developed.

1931 Japanese invade Manchuria.

1932 James Chadwick, English physicist, proves the existence of the neutral particle of the atom's nucleus, called the neutron. It proves to be by far the most useful particle for initiating nuclear reactions.

1932 Werner Heisenberg wins the Nobel Prize in physics for the creation of quantum mechanics, which has led to the discovery of the allotropic forms of hydrogen.

1932 Aldous Huxley publishes the novel *Brave New World,* which presents a dystopian view of genetic manipulations of human beings.

1932 The BOI starts the international exchange of fingerprint data with friendly foreign governments. Later halted as war approached, the program was not reinstituted until after World War II.

1932 In response to the Lindbergh kidnapping case and other high-profile cases, the Federal Kidnapping Act is passed to authorize BOI to investigate kidnappings perpetrated across state borders.

1932 Iraq declared an independent state.

1932 BOI establishes technical laboratory.

1933 In January, Adolf Hitler and Nazi Party take power in Germany. By the end of the year, Hitler proclaims Third Reich.

1933 U.S. president-elect Franklin D. Roosevelt escapes assassination attempt in Miami.

1933 Gilbert Newton Lewis, American chemist, is the first to prepare a sample of water in which all the hydrogen atoms consist of deuterium (the heavy hydrogen isotope). Called "heavy water," this will later play an important role in the production of the atomic bomb.

1934 Frédéric Joliot-Curie and Irène Joliot-Curie, a husband-and-wife team of French physicists, discover what they call *artificial radioactivity*. They bombard aluminum to produce a radioactive form of phosphorus. They soon learn that radioactivity is not confined only to heavy elements like uranium, but that any element can become radioactive if the proper isotope is prepared. For producing the first artificial radioactive element they win the Nobel Prize in chemistry the next year.

1934 John Marrack begins a series of studies that leads to the formation of the hypothesis governing the association between an antigen and the corresponding antibody.

1934 In an attempt to reduce organized crime violence, the U.S. Congress passes the National Firearms Act, which places restrictions on the sale of certain weapons favored by gang members.

1935 German Nazi party formalizes anti-Semitism with passage of Nuremberg laws.

1935 In violation of the Versailles Treaty, Germany begins to rearm and reconstitutes the German Air Force (Luftwaffe).

1935 Federal Bureau of Narcotics, forerunner of the modern Drug Enforcement Administration (DEA), begins a campaign portraying marijuana as a drug that leads to addiction, violence, and insanity. The government produces films such as *Marihuana* (1935), *Reefer Madness* (1936), and *Assassin of Youth* (1937).

1935 Irish Protestants in Belfast riot against Catholics, provoking Catholic retaliation.

1935 Patrick Maynard Stuart Blackett, English physicist, demonstrates that when gamma rays pass through lead, they sometimes disappear and give rise to a positron and an electron. This is the first demonstrable case of the conversion of energy into matter and as such, is a confirmation of Einstein's famous $E=mc^2$ equation.

1935 Robert Watson-Watt develops design for RADAR.

1935 Italian forces invade Ethiopia. The League of Nations, formed after World War I as an international body to ensure stability, fails to act.

1935 The BOI officially becomes the Federal Bureau of Investigation (FBI) on July 1.

1936 Spanish Civil War begins and becomes an international battleground pitting Francisco Franco's Fascist right against Marxist republican forces. Germany and Italy support Franco, while Soviet Union backs republicans. War will end with Franco's victory in 1939.

1936 Joseph Stalin begins a ''great purge.'' Lysenkoism, a repressive pseudoscientific set of beliefs, also begins to gain strength in Soviet politics.

1936 Sulphonamides, a class of antibiotics, introduced.

1936 Adolf Hitler includes synthetic fuel production as a priority in his Four-Year Plan.

1936 Eugene Paul Wigner, Hungarian-American physicist, proposes the theory of neutron absorption which comes into play when nuclear reactors are built.

1936 Germany reoccupies the Rhine River area, a key move toward later expansion in Europe.

1936 Italy and Germany sign Axis Pact, to which Japan will become a signatory in 1940.

1936 President Roosevelt asks FBI to report on the activities of Nazi and communist groups.

1937 Italy withdraws from the League of Nations to join a Germany-Japan pact.

1937 Emilio Segre, Italian-American physicist, and Carlo Perrier bombard molybdenum with deuterons and neutrons to produce element 43, technetium. This is the first element to be prepared artificially that does not exist in nature.

1937 William Thomas Astbury, English physicist, first obtains information about the structure of nucleic acids by means of x-ray diffraction.

1937 Japan invades eastern China.

1938 German Nazis attack Jews and Jewish businesses during night of violence termed *Kristallnacht.*

1938 Hitler annexes Austria.

1938 At Munich conference in September, Germany, backed by Italy, gains title to the Sudetenland in western Czechoslovakia. Britain, led by Prime Minister Neville Chamberlain, and France, comply in this act of diplomatic conquest. After appeasing Hitler, Chamberlain returns to Britain and proclaims, "Peace in our time!"

1938 Otto Frisch and Lise Meitner advance theory of uranium fission.

1938 Swiss chemist Albert Hofmann at Sandoz Laboratories synthesizes LSD. After initial testing on animals, Hoffman's subsequent accidental ingestion of the drug in 1943 reveals LSD's hallucinogenic properties.

1938 German scientists develop sarin while researching pesticides.

1938 The House Un-American Activities Committee (HUAC; sometimes called the Dies Committee) is initially charged with ferreting out Nazi activity in the United States but also begins to attempt to investigate Communist activity.

1938 Orson Welles' radio drama based on H.G. Wells' novel *War of the Worlds* causes panic among listeners who believe Martians have invaded Earth.

1938 Debut of the Minox camera, designed by Walter Zapp of Latvia, which was destined to become one of the most widely used miniature cameras by intelligence services on both sides of the iron curtain.

1939 In Vietnam, Ho Chi Minh creates the Viet Minh party to oppose French colonialism.

1939 Ernest Chain and H.W. Florey refine the purification of penicillin, allowing the mass production of the antibiotic.

1939 President Roosevelt assigns responsibility for investigating espionage, sabotage and other subversive activities jointly to the FBI, the Military Intelligence Service of the War Department (MID), and the Office of Naval Intelligence (ONI).

1939 Leo Szilard, Hungarian-American physicist, and Canadian-American physicist Walter Henry Zinn confirm that fission reactions (nuclear chain reactions) can be self-sustaining using uranium.

1939 Marguerite Perey, French chemist, first isolates element number 87 from among the breakdown products of uranium. She names it francium, after her country.

1939 Niels Bohr, Danish physicist, proposes liquid-drop model of the atomic nucleus and offers his theory of the mechanism of fission. His prediction that it is the uranium-235 isotope that undergoes fission is proved correct when work on an atomic bomb begins in the United States.

1939 Otto Hahn and Fritz Strassman publish results in which they observe that fission reactions can be self-sustaining because of the chain reaction that occurs.

This discovery eventually makes the construction of an atomic bomb feasible.

1939 Paul Hermann Müller, Swiss chemist, discovers the insect-killing properties of DDT (dichlorodiphenyltrichloroethane). It is used during WW II to kill disease-carrying lice, fleas, and mosquitoes, and after the war to kill agricultural pests. It is later proved to be a harmful environmental pollutant and its use in the United States is banned in 1972.

1939 Richard Brooke Roberts, American biophysicist, discovers that uranium fission does not release all the neutrons it produces at one time. This phenomenon of *delayed neutrons* eventually proves to be an important element in the safety of nuclear reactors.

1939 U.S. Geological Survey strategic mineral program started.

1939 The little-known tank battle at Nomonhan in August discourages Japanese hopes of easy victory against Soviets—a major factor motivating the Japanese refusal to join Germans in attacking Soviet Union two years later.

1939 Nazi Germany and Soviet Union sign Non-Aggression Pact on August 23.

1939 Albert Einstein sends a letter to President Roosevelt informing him of German atomic research and the potential for the development of an atomic bomb.

1939 World War II begins with the German invasion of Poland on September 1. Britain and France declare war on Germany.

1940 Germany launches a full-scale air war against England and extends persecution of the Jews into Poland, Romania, and the Netherlands.

1940 Winston Churchill succeeds Neville Chamberlain as Britain's prime minister.

1940 Ernest Chain and E.P. Abraham detail the inactivation of penicillin by a substance produced by *Escherichia coli*. This is the first bacterial compound known to produce resistance to an antibacterial agent.

1940 Leon Trotsky is assassinated in Mexico City by agents of SMERSH (*SMERrt SHpionam* or "Death to Spies").

1940 The British begin to intercept German non-Morse teleprinter text that used the Baudot Code, an international standard where each letter is represented by five binary elements.

1940 The FBI participates in the growing Red Scare by conducting additional arrests of suspected Communist agents under powers granted by the 1940 Smith Act, which permits the arrest of any individual inciting the overthrow of the government.

1940 The FBI establishes a Special Intelligence Service (SIS).

1941 The Lend-Lease Act allows the United States to send military supplies to Britian and other allies.

1941 Arnold O. Beckman, American physicist and inventor, invents the spectrophotometer. This instrument measures light at the electron level and can be used for many kinds of chemical analysis.

1941 Glenn Theodore Seaborg, American physicist, and his colleagues prepare the transuranium element 94, plutonium.

1941 Fairbairn-Sykes fighting knife first produced and used by Allies in World War II.

1941 U.S. Army Air Corps becomes Army Air Force. Six years later, the National Security Act of 1947 will transform this group into a full military service, the U.S. Air Force.

1941 On June 22, Germany launches largest land invasion in history against Soviet Union. Initial German efforts will meet with success, but three Russian winters, combined with Russian resistance, will result in German defeat by early 1944.

1941 U.S. president Roosevelt appoints William J. (Wild Bill) Donovan as Coordinator of Information, a proto intelligence service.

1941 On December 7, the Japanese attack the U.S. naval base at Pearl Harbor, Hawaii. In response, the United States enters World War II. The FBI is authorized to act against dangerous enemy aliens and to seize enemy aliens and contraband (e.g. short-wave radios, dynamite, weapons, and ammunition).

1942 German Nazi party makes Jewish extermination a systematic state policy, termed the "Final Solution."

1942 In the United States, economic depression is relieved by war production of planes, tanks, and other military supplies.

1942 The largest detainment of American citizens in the name of national security (ultimately resulting in the internment of 110,000 Japanese-Americans during World War II) begins two months after the Japanese attack on Pearl Harbor. The U.S. Department of Justice orders the detention of about 2,200 Japanese, 1,400 German, and 269 Italian nationals. More than 47,000 Issei (Japanese-born residents) are barred under federal law from gaining American citizenship, and 80,000 of their American-born family members, called Nissei, are subject to internment under Executive Order 9066, signed by President Roosevelt in February.

1942 Despite early losses in the war, Allied forces rally, defeating German Field Marshal Erwin Rommel in North Africa.

1942 Office of Strategic Services formed by President Roosevelt and led by William J. Donovan.

1942 Alcohol Tax Unit (ATU) formed and given responsibility for enforcing the Firearms Act.

1942 The U.S. military creates the Army-Navy Communications Intelligence Board (ANCIB).

1942 The Manhattan Project is formed to secretly build the atomic bomb before the Germans.

1942 Enrico Fermi, Italian-American physicist, heads a Manhattan Project team at the University of Chicago that produces the first controlled chain reaction in an atomic pile of uranium and graphite. With this first self-sustaining chain reaction, the atomic age begins.

1942 Frank Harold Spedding, American physicist, develops the necessary methods to produce pure uranium in very large quantities for the U.S. atomic bomb effort. Spedding's laboratory produces two tons in November, to be used for the first "atomic pile."

1942 The Clinton Engineer Works is built in Oak Ridge, Tennessee (later renamed the Oak Ridge National Laboratory). The Clinton Pile, the first true plutonium production reactor, begins operation in November 1943.

1942 Harvard University chemist Louis F. Fieser invents napalm.

1942 U.S. Geological Survey establishes military geology branch.

1942 Selman Waksman suggests that the word "antibiotics" be used to identify antimicrobial compounds that are made by bacteria.

1942 British Government Code and Cypher School (GC&CS) renamed the Government Communications Headquarters (GCHQ) to conceal its cryptologic mission.

1942 U.S. Naval intelligence breaks the Japanese navy's JN–25 code, providing valuable intelligence from the Battle of Midway to the end of World War II.

1942 U.S. naval victories against Japan in the naval battles of the Coral Sea in May and Midway in June. Fought primarily with carriers and aircraft, the first of these marks history's first naval battle in which opposing fleets' ships never came in sight of one another.

1942 Four German saboteurs come ashore from a U-boat on the beach near Amagansett, Long Island. Within the week, a second team of German saboteurs lands in Florida. Some saboteurs surrender and within two weeks the FBI captures the others.

1943 Mussolini overthrown and arrested on July 25; Prime Minister Pietro Badoglio, who has secretly been in contact with Allies, becomes Italian leader. Italy surrenders to the Allies. Mussolini is later rescued in a daring German airborne raid on September 12. He will spend the remainder of the war (and his life) as head of a puppet government based in the northern Italian town of Salo.

1943 The Soviet army defeats German troops at Stalingrad.

1943 Stalin abolishes the Soviet Comintern and the KGB and GRU (Soviet Army Intelligence) assume all espionage activities.

1943 J. Robert Oppenheimer, American physicist, is placed in charge of U.S. atomic bomb production at Los Alamos, New Mexico. He supervises the work of 4,500 scientists and oversees the successful design construction and explosion of the bomb.

1943 Lars Onsager, Norwegian-American chemist, works out the theoretical basis for the gaseous-diffusion method of separating uranium-235 from the more common uranium-238. This is essential for producing a nuclear bomb or nuclear power.

1943 First operational nuclear reactor is activated at the Oak Ridge National Laboratory in Oak Ridge, Tennessee.

1943 Construction starts (completed 1945) at the Hanford Site in Richland, Washington, where plutonium is to be produced.

1943 Colossus Mark I, the world's first programmable computing machine, built.

1943 Lockheed establishes its advanced development programs headquarters at Palmdale, California. Over the years that follow, this facility, known as the "Skunk Works," will be the birthplace of extraordinary aircraft such as the U-2, the SR-71, and the F-117A.

1943 U.S. Army renames SIS as the Signal Security Agency, or SSA.

1943 The SZ43 cipher machine is first used by Germany in WWII. The German military did not replace Enigma with the SZ42 for general use because the SZ42's complexity made it too heavy for the field.

1943 On January 15, just 16 months after the September 11, 1941, groundbreaking, the new Pentagon building is dedicated in Washington, D.C.

1943 U.S. Army's Signal Intelligence Service, a forerunner of NSA, formally begins program codenamed VENONA to break encrypted Soviet diplomatic communications.

1943 Amy Elizabeth Thorpe, a U.S. born British spy known as "Cynthia" acts as World War II's "Mata Hari."

1944 To combat battle fatigue during World War II, nearly 200 million amphetamine tablets are issued to U.S. soldiers stationed in Great Britain during the war.

1944 Massive Allied invasion of European continent at Normandy in France on June 6 (D Day). Invasion, under the command of General Dwight D. Eisenhower, is preceded by deception effort designed to convince Germans that the action will occur elsewhere.

1944 Allies liberate France, allow French troops under de Gaulle to ceremonially enter Paris first. Nazi puppet government at Vichy, France, collapses.

1944 Assassination attempt on Hitler and several other high-ranking officials. Himmler suspects that the plot was the work of agents inside of the government, most especially the Abwehr.

1944 Colossus II computer becomes operational.

1944 Otto Hahn receives the Nobel Prize in chemistry for his discovery of nuclear fission.

1944 Soviet Viktor Kravchenko defects to United States.

1944 Stalin orders creation of Department S, which will use American scientists as Russian spies.

1944 Britain's MI6 establishes a section devoted to Soviet espionage and subversion. Unfortunately, its director is Harold (Kim) Philby, a Soviet agent.

1945 Yalta Summit sets forth terms of a divided postwar Europe.

1945 U.S. troops liberate Nazi concentration camp at Buchenwald.

1945 Italian dictator Benito Mussolini killed by partisans on April 28, Adolf Hitler commits suicide April 30, and

Germany surrenders to the Allies on May 7. Germany is divided and occupied by the United States, the Soviet Union, Great Britain, and France.

1945 First atomic bomb is detonated by the United States at Trinity test site near Almagordo, New Mexico. The experimental bomb generates an explosive power equivalent to 15–20 thousand tons of TNT. The United States then destroys the Japanese city of Hiroshima with a nuclear fission bomb based on uranium-235 on August 6. Three days later a plutonium-based bomb destroys the city of Nagasaki. Japan surrenders on August 14 and World War II ends. This is the first use of nuclear power as a weapon.

1945 U.S. Department of State intelligence experts join Army-Navy Communications Intelligence Board (ANCIB) to form combined State-Army-Navy Communications Intelligence Board (STANCIB).

1945 United States develops a radar-absorbent paint containing iron.

1945 Army Security Agency (ASA) begins to provide the U.S. Army with signal intelligence and security information (ASA operates until 1976).

1945 OSS is abolished; operations transfer to its successor, Central Intelligence Group (CIG).

1945 League of Arab States formed; United Nations (UN) is created on October 24.

1946 In a January 22 presidential directive, President Harry S. Truman first uses the term "Director of Central Intelligence" (DCI) which he designates as the lead position in the CIG within the National Intelligence Authority (NIA). NIA will be abolished, and the DCI will eventually lead the Central Intelligence Agency (CIA).

1946 U.S. diplomat George Kennan's "Long Telegram" provides the ideological foundation for postwar policy toward the Soviet Union. Referring to the repressive Soviet domination of the Eastern Bloc states, British former prime minister Winston Churchill states that an "iron curtain" has come down across Europe.

1946 The organizational structure of the Royal Canadian Mounted Police is changed in response to the increased need for national security in Canada. Personnel are assigned to the Special Branch, which deals specifically with issues of national security.

1946 State-Army-Navy Communications Intelligence Board (STANCIB) becomes the U.S. Communications Intelligence Board (USCIB). FBI intelligence officers join the working group.

1946 In a postwar reorganization of the U.S. Army, the Military Intelligence Division is placed over the Army Security Agency and the Counter Intelligence Corps.

1946 U.S. Air Force Strategic Air Command (SAC) established at Offutt Air Force Base in Nebraska. It eventually becomes the command center for the defense "triad": the strategic bombers and ICBMs (intercontinental ballistic missiles) of the Air Force, and the U.S. Navy's submarine-launched ballistic missiles.

1946 On March 5, United States and United Kingdom sign UKUSA agreement, which brings together signals intelligence efforts of U.S., British, Canadian, Australian, and New Zealand agencies.

1946 American Electronic Numerical Integrator and Computer (ENIAC), is completed by the U.S. Army. ENIAC is considered the world's first computer until information on Colossus was finally declassified in the 1970s.

1946 Establishment of Bureau of Intelligence & Research, intelligence arm of U.S. State Department.

1946 U.S. Army School of the Americas established in Panama.

1946 Baruch Plan for international control of atomic weapons presented to the UN.

1946 The United States tests a nuclear bomb on Bikini Atoll, an island in the Pacific.

1946 In August, Congress passes the Atomic Energy Act, creating Atomic Energy Commission, and makes FBI responsible for investigating persons having access to restricted nuclear data. The FBI will also be responsible for investigation of criminal violations of this act.

1946 First Vietnam war, between Viet Minh and France, begins December 19.

1947 Voice of America begins regular radio broadcasts to Russia from transmitters in Munich, Manila, and Honolulu in February.

1947 William Shockley, John Bardeen, and Walter Brattain invent the transistor.

1947 Vice-President Richard Nixon speaks in Congress, attacking Gerhart Eisler, who had been revealed as a German communist spy and who was then being detained on Ellis Island for passport fraud and refusing to testify before HUAC. The House agrees with Nixon and votes a contempt charge, but Gerhart escapes to East Germany as a stowaway.

1947 The Taft-Hartley Act of 1947 bans members of the Communist Party from holding leadership positions in American labor unions.

1947 Three "pillars" of the containment policy are in place: Truman Doctrine (March 12), Marshall Plan (June 5), National Security Act (July 28). Supporting instruments include DOD, CIA, SAC, advance bases in Turkey and Libya. Stalin creates the Cominform, or Information Bureau of Communist parties, in August, at the meeting in Poland of the Soviet, East European, French and Italian communist parties. Andrei Zhadov reports to the conference that America and Russia are locked in a two-camp struggle for world domination.

1947 Major Charles E. "Chuck" Yeager breaks the sound barrier in a Bell XS-1 rocket-powered research plane in October.

1947 HUAC subpoenas 41 witnesses in an investigation of communism in Hollywood films. Ten witnesses who refuse to testify are jailed for contempt; supporters sign an *amici curiae* Supreme Court brief and many are subsequently refused work in the film industry.

1947 The UN proposes a division of what is now Israel almost equally between Israelis and Arabs. Arab countries reject this proposal.

1947 On December 19, the National Security Council gives the CIA orders to conduct its first covert operation, influencing the general elections in Italy to prevent a Communist victory. The operation is successful, resulting in victory for the Christian Democrat party in 1948.

1948 Soon after Israel becomes a state in May, it is attacked by Egypt, Iraq, Jordan, and Syria. Though outnumbered, the Israelis defeat the Arab nations, and Israeli territory expands to encompass an area larger than that allotted in the original UN partition.

1948 NSC directive creates Office of Policy Coordination to conduct covert operations for the CIA. Former Wehrmacht officer Reinhard Gehlen is recruited to carry out espionage against Russia in Eastern Europe. Gehlen warns the CIA about the coming blockade of Berlin but is ignored.

1948 The United States organizes the Berlin airlift to break the blockade of Berlin (entirely within the Soviet sector of Germany) imposed by Soviets.

1948 Czech Foreign Minister Jan Masaryk is killed in a "fall" from his office window following a communist coup on February 25.

1948 Yugoslavia expelled from the Cominform.

1948 DPRK (North Korea) established.

1948 Executive Order 9835 establishes Federal Employee Loyalty Program. FBI begins background investigations and refers questionable cases to loyalty boards. Federal employees are subject to dismissal for specific acts including disclosure of confidential information and association with subversive organizations.

1948 Congress creates the Air Force Office of Special Investigations.

1948 Nuclear tests in the South Pacific (Operation Sandstone) pave the way for mass production of weapons that previously had to be assembled by hand. By late 1948, the United States has 50 nuclear bombs.

1948 Indictments issued against leaders of the U.S. Communist Party for violation of Smith Act (advocating violent overthrow of the government).

1948 Germanium crystals are used by the Bell Telephone Company in the United States to build the first transistors.

1948 World Health Organization (WHO) formed. The WHO subsequently becomes the principal international organization managing public health related issues on a global scale. Headquartered in Geneva, the WHO will eventually become an organization of more than 190 member countries, contributing to international public health in areas including disease prevention and control, promotion of good health, vaccination programs, and development of treatment and prevention standards.

1948 Alger Hiss testifies that he has never been a communist, never participated in espionage, and does not know Whittaker Chambers. Chambers, a former communist and editor for *Time* magazine previously testified to the HUAC that Hiss had once supplied him with stolen documents. Chambers then produced microfilm of secret documents hidden inside a pumpkin on his Maryland farm. Hiss is indicted on charges of perjury. Eventually he is convicted and serves a prison sentence.

1949 Victory of Mao Zedong in China forces Nationalist government to flee to Formosa, where it establishes the Republic of China. Meanwhile, the world's largest population falls under communist rule as the People's Republic of China.

1949 FDA publishes "black book" guide to toxicity of chemicals in food.

1949 Armed Forces Security Agency established to coordinate military communications intelligence and security activities.

1949 Federal Republic of Germany (West Germany) and German Democratic Republic (East Germany) are established.

1949 In April, ten countries (Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal) join the United States and the United Kingdom to form the North Atlantic Treaty Organization (NATO).

1949 Judith Coplon becomes the first U.S. citizen convicted as a spy, a conviction that was later reversed because of illegal FBI wiretaps.

1949 May 12, the Soviets finally lift the blockade on Berlin. Train and auto transport resumes into the city. Allied Airlift operations continue through September until supplies regularly reach Berlin via train and truck.

1949 The Central Intelligence Agency Act of 1949 provides special administrative authorities and responsibilities for the agency and the director.

1949 Russia announces that its first A-bomb was successfully tested July 14.

1949 The CIA-sponsored Radio Free Europe begins broadcasting to Soviet-controlled Eastern Europe.

1950 Puerto Rican nationalists attempt to assassinate President Truman. As a result of this incident, in which a Secret Service agent is killed, Congress greatly expands the duties of the Secret Service.

1950 President Truman orders the Atomic Energy Commission to begin work to develop the hydrogen bomb (H-bomb).

1950 Wisconsin senator Joseph McCarthy launches an effort to identify and eliminate communism in America. "McCarthyism" is used to describe McCarthy's tactics of public denunciation without proof and forcing testimony through intimidation.

1950 British security agents in February arrest Los Alamos physicist Klaus Fuchs after an investigation based on an FBI tip derived from Soviet telegrams decrypted and decoded by the Army Signals Agency with FBI investigative assistance.

1950 East German government, with the assistance of the Soviet intelligence community, establishes the Stasi.

1950 The FBI initiates the Ten Most Wanted Fugitives Program in May in order to draw national attention to dangerous criminals who have avoided capture.

1950 McCarran Internal Security Act enacted, mandating that all communist organizations must register with the attorney general. The act also prohibits communists from working in national defense and prevents those who are members of "totalitarian" organizations from entering the United States.

1950 North Korea invades South Korea, igniting the Korean War. U.S. military troops sent to expel North Korean forces as part of a UN coalition.

1950 Determined to create a framework and mechanism for the production of reliable intelligence estimates, General Walter Bedell Smith, when he becomes Director of Central Intelligence in October, institutes the concept and practice of developing national intelligence estimates.

1950 Arrest of Julius and Ethel Rosenberg, who are tried, convicted, and later executed for espionage against the United States.

1950 MacArthur crosses the 38th parallel in an attempt to liberate North Korea.

1950 President Truman escapes assassination attempt unhurt as two Puerto Rican nationalists shoot their way into Blair House in Washington, D.C. Officer Leslie Coffelt, of the White House police, is shot and killed. In response, Congress enacts legislation the following year that permanently authorizes Secret Service protection of the president, his immediate family, the president-elect, and the vice president.

1950 North Korean troops gain easy victories against UN forces, but when MacArthur launches a bold offensive at Inchon, he cuts the North Korean army in half. By Thanksgiving, he promises that U.S. troops will be home by Christmas, but on November 25, China enters the war, and drives the UN forces back to the 38th parallel. Allied bombing ensures that this line remains the boundary between North and South Korea.

1951 In *Dennis v. U.S.,* the Supreme Court upholds decisions declaring U.S. Communist Party illegal because the party constitutes a "clear and present danger." The Court reverses itself in 1957.

1951 The United States forms a special committee to analyze the nation's intelligence and cryptographic efforts. The committee is, in part, composed of the secretaries of state, defense, and the DCI (CIA director). Later in the year, President Truman issues a top-secret directive creating the National Security Agency (NSA).

1951 Mossad, Israel's chief intelligence collection, counterterrorism, and covert action agency, established on April 1.

1951 CIA is given responsibility to determine the overall requirements of foreign economic intelligence.

1951 General MacArthur, eager for victory against the Chinese in Korea, attempts to defy President Truman's orders to stand down, and calls for American citizens' support of his plan to invade China. For this act of insubordination, Truman relieves him of duty on April 11, and replaces him with General Matthew B. Ridgway.

1951 The first usable electricity from nuclear fission is produced.

1952 British scientists develop VX nerve agent while studying insecticides.

1952 First thermo-nuclear device is exploded successfully by the United States at the Eniwetok Atoll in the South Pacific. This hydrogen-fusion bomb (H bomb) is the first such bomb to work by nuclear fusion and is considerably more powerful than the atomic bomb exploded over Hiroshima on August 6, 1945.

1952 First use of isotopes in medicine.

1952 The Treasury Department's Bureau of Internal Revenue (BIR) becomes the Internal Revenue Service (IRS). BIR's Alcohol Tax Unit—latest in a series of offices through which Treasury has enforced federal alcohol, tobacco, and firearms policy over the years—becomes the IRS Alcohol and Tobacco Tax Division.

1952 Greece and Turkey join NATO.

1952 First U.S. overflights of Soviet airspace, using B-47 Stratojets.

1952 In National Security Council Intelligence Directive (NSCID) No. 9, a secret memorandum issued on October 24, President Truman establishes the U.S. National Security Agency (NSA).

1952 McCarran-Walter Act is revised. The new immigration quota laws allow more Asians but exclude "subversives" and give the attorney general the right to deport immigrants found to be communists even after they acquired U.S. citizenship.

1952 Great Britain explodes its first nuclear device.

1953 Joseph Stalin dies and a political power struggle starts in the U.S.S.R.

1953 James D. Watson and Francis H. C. Crick publish two landmark papers in the journal *Nature*. The papers are titled "Molecular Structure of Nucleic Acids: A Structure for Deoxyribose Nucleic Acid" and "Genetic Implications of the Structure of Deoxyribonucleic Acid." Watson and Crick propose a double helical model for DNA and call attention to the genetic implications of their model. Their model is based, in part, on the x-ray crystallographic work of Rosalind Franklin and the biochemical work of Erwin Chargaff. Their model explains how the genetic material is transmitted.

1953 U.S. Federal Security Agency becomes the Department of Health, Education, and Welfare (HEW).

1953 United States receives information on VX nerve agent production from United Kingdom and sets up lab in Edgemont, Maryland to study it.

1953 U.S. president Dwight D. Eisenhower delivers "Atoms for Peace" speech to the UN, calling for the creation of an organization to control and develop the use of atomic energy. He later publicly predicts the potential for a nuclear arms race between the United States and the Soviet Union.

1953 An armistice on July 27 brings an end to the Korean War.

1953 In August, Operation AJAX, conducted by British and American intelligence, deposes Iraqi prime minister Mohammad Mossadegh, and restores Shah Mohammad Reza Pahlavi to the throne.

1954 CIA-supported coup in Guatemala overthrows President Jacobo Arbenz.

1954 U.S. policy of massive retaliation to any Communist aggression (forerunner of MAD—Mutually Assured Destruction—policy).

1954 French garrison at Dien Bien Phu falls to Viet Minh on May 7, and in July, French agree to leave Vietnam.

1954 Site-R, an underground government communications and operations facility in Pennsylvania, is completed.

1954 U.S. Navy commissions its first nuclear sub, *Nautilus,* on September 30.

1954 Televised Army-McCarthy hearings. Senator McCarthy focuses his hunt for communists on the highest echelons of the military, is finally denounced for his unscrupulous tactics, and is ultimately censured by the Senate.

1954 Manhattan Project physicist Robert Oppenheimer is stripped of his security clearance and is dismissed from government service, suspected of being a communist sympathizer.

1954 Atomic Energy Act is passed.

1954 Communist Control Act is passed, briefly outlawing the Communist Party in the United States.

1955 West Germany joins NATO. The Soviet Union and eight Eastern European states respond by forming the Warsaw Pact.

1955 National Institutes of Health organizes a Division of Biologics Control within FDA, following a death caused by a faulty polio vaccine.

1955 Cesium atomic clock developed.

1955 Boeing B-52 Stratofortress introduced.

1955 U.S. Navy Fleet Intelligence Center Pacific (FICPAC) established.

1955 ASA expands its mission to include electronic intelligence and electronic warfare functions that had formerly been the responsibility of the signal corps. Because its role now encompasses more than intelligence and security, it is reassigned from G-2 (military intelligence) to the U.S. Army Chief of Staff.

1955 The Berlin tunnel (operational from March 1955 until its discovery by Soviet troops in April 1956) allowed Western intelligence agencies to tap Soviet and East German communications.

1955 President Eisenhower signs a bill authorizing $46 million for construction of a CIA Headquarters Building.

1955 A United Airlines DC-6B explodes near Longmont, Colorado, on October 1, killing all 39 passengers and 5 crewmembers. The FBI provides assistance from its Disaster Squad in identifying the deceased.

1955 In December, U.S. Air Force launches Project GENETRIX, a surveillance operation using balloons over communist countries. The unsuccessful effort comes to an end three months later.

1955 President Eisenhower sends first U.S. military and civilian advisers into Vietnam, which in 1955 is divided into northern and southern portions.

1956 President Eisenhower establishes the President's Board of Consultants on Foreign Intelligence Activities, predecessor to the President's Foreign Intelligence Advisory Board.

1956 First U-2 overflight of Soviet Union on July 5.

1956 Hungarian revolution is crushed by Soviet military.

1956 Suez Crisis when Western powers, worried over Egyptian president Gamal Abdel Nasser's close ties with the Soviet bloc, refuse assistance in building Aswan High Dam. In response, Nasser seizes the Suez Canal. Britain and France form an alliance with Israel, which invades on October 26.

1956 Fidel Castro launches Cuban revolution against the Batista regime.

1956 Soviet First Secretary Nikita Khrushchev, speaking about the West, states "History is on our side. We will bury you." The following year, he becomes premier of the Soviet Union.

1956 Pakistan officially becomes an Islamic state.

1957 International Atomic Energy Agency (IAEA) is formed as an autonomous UN body to verify that nuclear materials are not used in a prohibited manner.

1957 In March, President Eisenhower proclaims the Eisenhower Doctrine, whereby "the United States regards as vital to the national interest and world peace the preservation of the independence and integrity of the nations of the Middle East."

1957 The Soviet Union launches *Sputnik.*

1957 Civil Rights Act of 1957 establishes U.S. Commission on Civil Rights.

1957 The sodium reactor experiment at Santa Susana, California, provides the first power generated from a civilian nuclear reactor.

1957 June 21, the FBI arrests Colonel Rudolf Ivanovich Abel, a Soviet espionage agent.

1957 United States conducts first underground nuclear test in a tunnel 100 miles from Las Vegas.

1958 U.S. National Defense Education Act dedicates resources to math, science, and language education.

1958 United States establishes NASA (the National Aeronautics and Space Administration).

1958 Explorer 1, the first U.S. satellite, launched with a cosmic ray detector onboard.

1958 U.S. Department of Defense establishes Advanced Research Projects Agency (ARPA).

1958 The Federal Aviation Act passes, creating the Federal Aviation Agency.

1958 Congress passes Defense Reorganization Act, which creates unified military commands within the U.S. Department of Defense.

1958 United States conducts nuclear tests high above the Pacific Ocean. The explosions send out an extremely high-frequency electromagnetic pulse that turns off street lights in Hawaii and disrupts radio navigation as far away as Australia for up to 18 hours.

1958 Iraqi monarchy is overthrown in a military coup.

1958 Following the Geneva Conference on the Discontinuance of Nuclear Weapons Tests, the United States, Great Britain, and Soviet Union declare temporary testing moratoriums.

1959 The microchip, forerunner of the microprocessor, is invented.

1959 Fidel Castro takes power in Cuba on January 1.

1959 Launch of the *Forrestal,* the first of many large carriers deployed by the U.S. Navy. The *Forrestal* includes rectangular extensions on the rear part of the flight deck, which greatly expand the deck area.

1959 U.S. Navy's Marine Mammal Program established near Los Angeles, CA.

1959 Discoverer XIV, the first successful mission of the Corona satellite program, which was developed the previous year to photograph sites in the Soviet Union. The returning capsule, containing 20 pounds of film and suspended from a parachute, is snatched from midair by a U.S. C-119 aircraft.

1959 President Eisenhower approves a secret program, proposed by the CIA, to depose communist Cuban leader Fidel Castro.

1960 Chinese criticisms of the Soviet Union cause a split in Sino-Soviet relations.

1960 Vietcong seek to overthrow South Vietnamese president Ngo Dinh Diem.

1960 First U.S. KeyHole intelligence satellite launched.

1960 Theodore Harold Maiman, American physicist, develops the first laser. He uses a ruby cylinder that emits a light that is coherent (all in a single direction) and monochromatic (a single wavelength). He finds that it can travel thousands of miles as a beam without dispersing, and that it can be concentrated into a small, super-hot spot. Laser is an acronym for Light Amplification by Stimulated Emission of Radiation.

1960 France explodes its first nuclear device.

1960 Premier Nikita Khrushchev vows the Soviet Union will support "wars of national liberation."

1960 The NSA begins intercepting messages and communications revealing the Soviet military buildup in Cuba, including the installation of air defense systems and missile capabilities.

1960 U.S. Navy Fleet Intelligence Center Europe (FICEUR) established.

1960 Defense Information Systems Agency (DISA) established as Defense Communications Agency.

1960 In September, NSA cryptographers William H. Martin and Bernon F. Mitchell defect to the Soviet Union and issue the first public revelations as to NSA's mission.

1960 A Soviet missile shoots down an American U-2 spy plane near Sverdlovsk. The pilot Francis Gary Powers is detained and tried by the Soviet Union as a spy. After nearly two years, Powers is exchanged for a captured Soviet spy. Soviet outrage over the incident leads to the collapse of the Paris summit of the Conference on Discontinuance of Nuclear Weapons Trials.

1961 In his inauguration speech, President John F. Kennedy sets the tone for modern U.S. foreign policy when he states, "Let every nation know, whether it wishes us well or ill, that we shall pay any price, bear any burden, meet any hardship, support any friend, oppose any foe to assure the survival and success of liberty."

1961 National Photographic Interpretation Center (NPIC) formed.

1961 U.S. Strategic Air Command activates its Airborne Command Post on February 3. Known as Looking Glass for the fact that equipment aboard its planes mirrors control systems on the ground, Looking Glass will remain in continuous operation for the next 29 years.

1961 Soviet Union launches first cosmonaut, Yuri Gagarin, into space.

1961 Cuba establishes what will become its largest intelligence agency, the Dirección General de Inteligencia (DGI; General Intelligence Directorate), within the Ministry of the Interior.

1961 Cuban exiles organized and armed by the CIA invade Cuba on April 17, in a failed attempt to overthrow the leftist leader Fidel Castro. The event became known as the "Bay of Pigs," in reference to the small bay on the southern coast of Cuba where the invasion commenced.

1961 Congress creates the U.S. Arms Control and Disarmament Agency (ACDA), devoted to policy making for conventional and nuclear armament.

1961 United States introduces the first nuclear-powered aircraft carrier, the *Enterprise.*

1961 First U.S. aircraft hijacking on May 1. The hijacker takes over the plane at gunpoint and forces pilots to fly to Havana, Cuba, where he is granted asylum.

1961 In August, the Soviet Union and East Germany erect the Berlin Wall to divide West and East Berlin.

1961 In a letter published in the September issue of *Life* magazine, President Kennedy advises Americans to build fallout shelters to reduce American vulnerability to Soviet nuclear attack. "Shelter-mania" ensues as Americans prepare for potential nuclear attack.

1961 Defense Intelligence Agency established.

1961 Soviet Union resumes nuclear weapons testing after dispute on verification provisions of test ban agreements. Two weeks later the United States resumes testing.

1962 Commissioning of the first Navy SEAL (sea, air, land) teams.

1962 Cuban missile crisis, triggered by the Soviet deployment to Cuba of medium-range, nuclear-armed ballistic missiles, brings the world to the brink of nuclear war. The United States blockades Cuba for 13 days until the Soviet Union agrees to remove its missiles. The United States also agrees to remove its missiles from Turkey. The crisis marks the first time the NSA creates an around-the-clock command center.

1962 During the Cuban Missile Crisis in October, President Kennedy becomes concerned with faulty communications technology in the national security communications apparatus. After the crisis ends, he calls for a study to improve communications coordination and technology, ultimately leading to the formation of the National Communication System.

1963 A nuclear submarine, the USS *Thresher,* sinks off the coast of Cape Cod in 8,400 feet of water, killing all 129 sailors aboard.

1963 Development of Canada Geographic Information System, the first modern geographic information system, begins.

1963 Coup in Iraq led by the Arab Socialist Ba'th Party (ASBP).

1963 Directorate of Science and Technology, the arm of the CIA responsible for technological development, is formed.

1963 Britain's war minister, Lord John Dennis Profumo, is discovered to be sleeping with Christine Keeler, who is also having an affair with a Soviet spy. The scandal becomes known as the Profumo affair.

1963 Israel's Mossad assists in the defection of an Iraqi airman, who delivers to Israel a Soviet MiG-21 fighter jet.

1963 The United States and Soviet Union set up a hotline (teletype) between the White House and the Kremlin.

1963 The United States and Soviet Union sign the Limited Test Ban Treaty, which prohibits underwater, atmospheric, and outer space nuclear tests. More than 100 countries have ratified the treaty since 1963.

1963 Assassination of South Vietnamese President Ngo Dinh Diem on November 1.

1963 November 22, Lee Harvey Oswald assassinates President Kennedy in Dallas, Texas. Lyndon B. Johnson becomes president.

1964 American refusal to fly the Panamanian flag over a high school in the Panama Canal Zone sparks riots that leave 23 Panamanians and four U.S. Marines dead. Afterward, Panama calls for new treaty discussions with the United States.

1964 U.S. Navy introduces E-2 Hawkeye airborne early warning and command and control aircraft.

1964 North Vietnamese gunboats open fire on U.S. destroyer *Maddox* in the Gulf of Tonkin on August 2. This results in the Gulf of Tonkin resolution, passed by U.S. Senate, which gives President Johnson power to vastly escalate U.S. commitment in Vietnam.

1964 China conducts its first nuclear test.

1965 American troops sent to the Dominican Republic to prevent a communist takeover.

1965 Congress passes Drug Abuse Control Amendments—legislation that forms the FDA Bureau of Drug Abuse Control and gives the FDA tighter regulatory control over amphetamines, barbiturates, and other prescription drugs with high abuse potential.

1965 Congress authorizes protection of former presidents and their spouses during their lifetime and minor children until age 16.

1965 In June, first U.S. ground troops arrive in Vietnam.

1965 Anthrax vaccine adsorbed (AVA), is approved for use in the United States.

1965 First bombings against Israel by the Palestine Liberation Organization (PLO).

1966 France withdraws its troops from the North Atlantic Treaty Organization (NATO). French President de Gaulle argues for a Europe free from both American and Soviet intervention.

1966 Marshall Nirenberg and Har Gobind Khorana lead teams that decipher the genetic code. All of the 64 possible triplet combinations of the four bases (the codons) and their associated amino acids are determined and described.

1966 NORAD Combat Operations Center in Cheyenne Mountain becomes fully operational.

1966 Naval Investigative Service, predecessor of the Naval Criminal Investigative Service, formed as an office within the Office of Naval Intelligence.

1967 FBI's National Crime Information Center (NCIC) becomes operational.

1967 Congress passes Freedom of Information Act, which limits the ability of U.S. federal government agencies to withhold information from the public by classifying that information as secret.

1967 In the Six-Day War, fought in the first week of June, Israel defeats a much larger Arab force, and gains control of the west bank of the Jordan River, which was previously Jordanian territory.

1967 CIA launches Phoenix program to fight Vietcong infrastructure in South Vietnam.

1967 A cosmic gamma ray burst leads to the discovery of a new phenomenon for astronomers to study. The burst is detected while U.S. Vela spy satellites remain alert for potential Soviet nuclear testing in space. Part of an unclassified research and development program, the Vela program was designed to develop nuclear monitoring technology. Vela satellites carried x-ray, gamma-ray, neutron detectors, EMP detectors and other instruments.

1968 An overwhelming North Vietnamese attack on South Vietnamese cities, called the Tet Offensive, ultimately proves to be a crucial psychological turning point in the Vietnam War.

1968 FDA administratively moves to Public Health Service.

1968 During testing exercise of VX nerve agent, 6,400 sheep are killed near Dugway, Utah.

1968 Following passage of the Gun Control Act, the Alcohol and Tobacco Tax Division of IRS becomes the Alcohol, Tobacco, and Firearms (ATF) Division.

1968 U.S. Navy Fleet Intelligence Center Atlantic (FICLANT) established.

1968 U.S. anti-drug agencies in the Treasury and Health, Education, and Welfare departments merged to form the Bureau of Narcotics and Dangerous Drugs under the Justice Department.

1968 National Institute of Justice established under the authority of the Omnibus Crime Control and Safe Streets Act to provide independent, evidence-based tools to assist state and local law enforcement.

1968 Creation of first national contingency plan to deal with oil spills in the United States.

1968 Israel's Mossad successfully captures eight missile boats that Israel had ordered from France, but which President Charles de Gaulle had placed under embargo. Mossad also captures and brings to trial nuclear technician Mordechai Vanunu, who had revealed Israeli nuclear secrets to the British press.

1968 Prague Spring reforms in Czechoslovakia ended by Soviet invasion.

1968 James Earl Ray assassinates Dr. Martin Luther King Jr. in Memphis, Tennessee, on April 4. The FBI opens a special investigation based on the violation of Dr. King's civil rights so that federal jurisdiction in the matter can be established.

1968 As a result of Senator Robert F. Kennedy's assassination on June 5, Congress authorizes protection of major presidential and vice-presidential candidates and nominees.

1968 Nuclear Nonproliferation Treaty (NPT)—calling for halting the spread of nuclear weapons capabilities—is signed.

1968 Final flight of X-15 hypersonic aircraft on October 24.

1969 President Richard Nixon begins troop withdrawal from Vietnam.

1969 On July 20, U.S. astronaut Neil Armstrong becomes the first man to walk on the moon.

1969 Strategic Arms Limitation Talks (SALT) begin between the United States and the Soviet Union.

1969 United States and Soviet Union begin period of diplomatic détente.

1969 By Executive Order, the United States renounces first-use of biological weapons and restricts future weapons research programs to issues concerning defensive responses (e.g., immunization, detection, etc.).

1969 Microprocessor developed.

1969 Defense Department's Advanced Research Projects Agency (ARPA) establishes ARPANET, a forerunner to the Internet.

1969 Muammar Qaddafi seizes power from King Idris in Libya on September 1.

1970 The National Environmental Policy Act of 1969 is signed, requiring the federal government to review the environmental impact of any action—such as construction of a building—that might significantly affect the environment.

1970 United States Congress passes Controlled Substance Act (CSA), delineating a hierarchy of commonly abused drugs and establishing corresponding penalties for misuse.

1970 United States Environmental Protection Agency established.

1970 White House Police Force renamed the Executive Protective Service.

1970 The UN assigns the International Atomic Energy Agency (IAEA) the task of NPT monitoring and for developing nuclear safeguards.

1970 The Consolidated Federal Law Enforcement Training Center, a bureau of the Department of the Treasury, is established as an organization to provide training for all federal law-enforcement personnel. Today known as the Federal Law Enforcement Training Center, it is now part of the Department for Homeland Security.

1970 In October, a group advocating the separation of Quebec from Canada kidnaps two government officials and murders one of them. The crisis causes the temporary imposition of martial law in the country and renews calls for a dedicated security agency.

1970 Congress approves the Organized Crime Control Act in October. This law contains a section known as the Racketeer Influenced and Corrupt Organization Act or RICO. RICO becomes an effective tool in convicting members of organized criminal enterprises.

1971 CIA activity in Laos, termed by critics a "secret war," is exposed.

1971 Chinese defense minister Lin Biao attempts a coup against Mao Zedong but is killed in a plane crash. China is officially seated in the UN and launches its first space satellite.

1971 Stolen by Defense Department official Daniel Ellsberg, a classified set of papers detailing compromising U.S. involvement in Vietnam, "The Pentagon Papers," is published by the *New York Times* and the *Washington Post*.

1971 United Kingdom passes the Misuse of Drugs Act.

1971 Canada Geographic Information System becomes operational.

1971 Congress authorizes Secret Service protection for visiting heads of a foreign state or government, or other official guests, as directed.

1971 The NSA receives operation control over the cryptologic agencies of the air force, army and navy. The three agencies are reorganized into the newly created Central Security Service (CSS) headed by the NSA director. The move centralizes the government's

signals intelligence (SIGINT) and communications security (COMSEC) programs under the NSA.

1971 Spy satellite called *Hexagon* is launched carrying a KH-9 camera.

1972 U.S. president Nixon meets with Mao Zedong in Beijing. The meeting eases U.S.-China animosities.

1972 President Nixon visits Soviet Union.

1972 United States and Soviet Union under Premier Leonid Brezhnev) negotiate reductions in nuclear arsenals.

1972 Defense Investigative Service (changed in 1997 to Defense Security Service) established on January 1.

1972 Recombinant technology emerges as one of the most powerful techniques of molecular biology. Scientists are able to splice together pieces of DNA to form recombinant genes. As the potential uses, therapeutic and industrial, become increasingly clear, scientists and venture capitalists establish biotechnology companies.

1972 *Landsat I* satellite launched, providing the first publicly available satellite imagery.

1972 Congress passes the Consumer Product Safety Act, creating the Consumer Product Safety Commission, which is charged with protecting the public from risk or injury involved with defective or unsafe products.

1972 The ATF Division of IRS becomes a separate Treasury bureau, the Bureau of Alcohol, Tobacco, and Firearms.

1972 Computer axial tomography, commonly known as CAT scanning, is introduced. A CAT scan combines many high-definition, cross-sectional x-rays to produce a two-dimensional image of a patient's anatomy.

1972 President Nixon issues Executive Order 11652, which stipulates that virtually all national security records should be declassified after 30 years.

1972 Five men ultimately discovered to have ties to anti-Castro forces, the American CIA, and the White House are arrested inside the Democratic National Headquarters at the Watergate Hotel in Washington, D.C. Known as a "plumbers" team, the intelligence operatives carried electronic surveillance equipment and cameras. A subsequent cover-up of the break-in, destruction of taped conversations related to the cover-up, and revelations of a history political dirty tricks form the core of the Watergate scandal that ultimately leads to criminal prosecutions of top officials and President Nixon's resignation in August 1974.

1972 The Antiballistic Missile (ABM) Treaty is signed by the United States and the Soviet Union. The treaty is one of two treaties produced by the first series of Strategic Arms Limitation Talks (SALT I) between the two countries; the other is an interim agreement limiting offensive nuclear weapons.

1972 U.S. Department of Defense directs Advanced Research Projects Agency (ARPA) name change to the Defense Advanced Research Projects Agency (DARPA) in March. DARPA is established as a separate defense agency under the Office of the Secretary of Defense.

1972 The FBI Academy opens a new training facility on the Marine Corps Base at Quantico, Virginia in May.

1972 Biological and Toxin Weapons Convention first signed. BWC prohibits the offensive weaponization of biological agents (e.g., anthrax spores). The BWC also prohibits the transformation of biological agents with established legitimate and sanctioned purposes into agents of a nature and quality that could be used to effectively induce illness or death.

1972 "Bloody Friday": on July 21, an IRA bomb attack kills 11 people and injures 130 in Belfast, Northern Ireland. Ten days later, three additional IRA attacks in the village of Claudy leave six dead.

1972 Establishment of U.S. Air Force Intelligence Service in June.

1972 After 11 Israeli athletes are murdered by Palestinian terrorists with the Black September organization at the Munich Olympics in September, Israel's Mossad establishes an action team, Wrath of God. Over the next two years, the team tracks down and kills a dozen members of Black September.

1972 Iraq and Soviet Union sign 15-year Treaty of Friendship and Cooperation.

1973 The peace treaty ending the Vietnam War, the Paris Peace Accords, is signed. South Vietnam collapses two years later after the last U.S. troops are withdrawn.

1973 Atmospheric Release Advisory Capability (ARAC) concept has its origins when the Department of Energy (DOE) seeks assistance from scientists at California's Lawrence Livermore National Laboratory in assessing potential and ongoing atmospheric hazards.

1973 Concerns about the possible hazards posed by recombinant DNA technologies, especially work with tumor viruses, leads to the establishment of a meeting at Asilomar, California. The proceedings of this meeting are subsequently published by the Cold Spring Harbor Laboratory as a book entitled *Biohazards in Biological Research.*

1973 Drug Enforcement Administration (DEA) created on July 1.

1973 Libya claims the Gulf of Sidra in defiance of international protocol.

1973 General Augusto Pinochet, with the support of the CIA, overthrows Marxist president Salvador Allende in Chile in September. Allende dies—either by suicide (according to Pinochet) or by murder (according to Allende's supporters).

1973 Arab-Israeli Yom Kippur War. Fourth Arab-Israeli war begins with a combined Egyptian and Syrian attack against Israel in October. When military efforts fail, the Organization of Petroleum-Exporting Countries (OPEC) announces a cutback in oil production, raising gasoline prices and precipitating an energy crisis in the United States.

1974 Congress passes the Energy Reorganization Act, which abolishes the Atomic Energy Commission (AEC) and replaces it with two other agencies: the Nuclear Regulatory Commission (NRC) and the Energy Research and Development Administration.

1974 Members of the Symbionese Liberation Army (SLA) kidnap heiress Patricia Hearst on February 5. Hearst, allegedly brainwashed by the group, adopts the name "Tania" and participates in bank robberies. Most members, including leader Donald DeFreeze, are killed in a May 1974 shootout with authorities, and Hearst is captured by the FBI in September 1975. In January 2001, outgoing president William J. Clinton pardons her.

1974 Treaty on Underground Nuclear Weapons Tests (also known as the Threshold Test Ban Treaty) is signed by the United States and Soviet Union, prohibiting underground nuclear weapons tests using weapons that produce yields greater than 150 kilotons.

1974 U.S. Navy Fleet Intelligence Center (FIC) Europe (FICEUR) and FIC Atlantic (FICLANT) merge to form FIC Europe-Atlantic (FICEURLANT).

1974 Cuba's National Liberation Directorate (DLN), which is responsible for fomenting communist revolutions worldwide, becomes the America Department (DA) of the Communist Party of Cuba Central Committee. During the years that follow, DA will provide support to communist insurgents and terrorists in numerous locales.

1974 Congress passes Privacy Act of 1974, greatly restricting the authority of agencies to collect information on individuals, or to disclose that information to persons other than the individual. The Privacy Act also requires agencies to furnish individuals with any information on them that the agency has in its files.

1974 New era of congressional oversight in intelligence begins with passage of Hughes-Ryan Act amending the Foreign Service Act. Written in the wake of covert activities that helped bring down the Marxist regime of Salvador Allende in Chile, Hughes-Ryan requires the president to submit plans for covert actions to the relevant congressional committees.

1974 The *New York Times* publishes a report concerning a CIA domestic intelligence campaign involving interception of private mail.

1974 India conducts its first nuclear test—an explosion in the Rajasthan Desert.

1974 British Prevention of Terrorism Act permits the arrest of suspected terrorists without a warrant and allows authorities to detain them for a week without bringing charges. While being interned, detainees are subject to a range of harsh practices that include "hooding"—being isolated and forced to wear a hood over their heads—noise bombardment, and sleep and food deprivation.

1974 Bar-coded products arrive in American stores, along with the laser scanners used at checkout stations to read the codes.

1975 American Apollo 18 and Soviet Soyuz 19 join in an orbital linkup.

1975 Puerto Rican nationalists bomb a Wall Street bar, killing four and injuring 60; two days later, the Weather Underground claims responsibility for an explosion in a bathroom at the U.S. Department of State in Washington.

1975 The duties of Executive Protective Service are expanded to include protection of foreign diplomatic missions located throughout the United States and its territories.

1975 U.S. Nuclear Emergency Support Team established to analyze and respond to cases involving nuclear threats.

1975 On April 30, Saigon falls to North Vietnamese. In the following year, Vietnam is united under a communist government.

1975 Commissioning, in May, of the *Nimitz,* first in a super-class of large modern aircraft carriers deployed by the U.S. navy.

1975 President Gerald R. Ford signs Executive Order 11828, creating the Commission on CIA Activities within the United States.

1975 Investigations by congressional committees headed by Idaho senator Frank Church and New York representative Otis Pike reveal that government agencies, including the NSA, performed clandestine surveillance on U.S. citizens who participated in the civil rights and anti-Vietnam War movements.

1975 FBI special agents Jack R. Coler and Ronald A. Williams are murdered while conducting an investigation on an Indian reservation in South Dakota. American Indian Movement leader Leonard Peltier is convicted of committing the murders.

1975 President Ford escapes an assassination attempt in Sacramento, California, by Lynette Alice (Squeaky) Fromme, who pointed a gun at him but did not fire. A few weeks later, Ford escaped another assassination attempt in San Francisco, California, when Sara Jane Moore was prevented from firing at him by a bystander.

1976 Chinese Premier Zhou Enlai and Central Committee Chairman Mao Zedong die.

1976 Church Committee submits its final report on April 26. Meanwhile, on January 29, just two days before the Pike Committee was to complete its investigation, the House votes not to make its findings public. (The report was later leaked to journalist Daniel Schorr, who passed it on to the *Village Voice*.)

1976 On May 19, the Senate establishes its permanent Select Committee on Intelligence. On July 14, 1977, the House puts in place its own such committee.

1976 On the night of July 3–4, members of Israel's Mossad conduct a raid on a French airliner, hijacked by Palestinian terrorists, in the Uganda city of Entebbe. The Israelis rescue all but four of the plane's 97 passengers, losing a single officer, along with 20 Ugandan soldiers, in the process.

1976 A military junta overthrows the government of Argentina.

1977 The United States vetoes a UN Security Council resolution calling for total Israeli withdrawal from Arab areas.

1977 U.S. ambassador Francis E. Melroy is killed in Beirut.

1977 U.S. president James E. Carter and Panamanian military dictator Omar Torrijos sign the Panama Canal Treaty on September 7, which abolishes the Canal Zone, terminates all prior treaties regarding the canal, and provides for the full transfer of the canal to Panama on December 31, 1999. A separate Neutrality Treaty guarantees the neutrality of the canal in perpetuity. Congress ratifies both treaties the following year.

1977 Introduction of E-3 Sentry AWACS (airborne warning and control system). Packed with electronics, the aircraft—based on the Boeing 707—serves purposes that include identifying enemy aircraft, jamming enemy radar, guiding bombers to their targets, and managing the flow of friendly aircraft.

1977 The last reported smallpox case recorded. Ultimately, the WHO declares the disease eradicated.

1977 Office of Intelligence Support (OIS) established as the intelligence office of the U.S. Department of the Treasury. OIS thus replaces Office of National Security, established in 1961.

1977 U.S. Army Intelligence and Security Command (INSCOM) goes into operation on January 1.

1977 In November, Delta Force is activated. Established by Colonel Charles Beckwith at Fort Bragg, North Carolina, Delta Force becomes one of the leading U.S. counterterrorist units.

1977 A new security and intelligence command known as Headquarters, U.S. Army Intelligence and Security Command, replaces ASA.

1977 Department of Energy Organization Act signed into law by President Carter on October 1. The U.S. Department of Energy (DOE) replaces the Energy Research and Development Administration and consolidates Federal energy programs and activities.

1978 The United States recognizes the People's Republic of China (PRC).

1978 On January 24, President Carter signs Executive Order 12036, "United States Foreign Intelligence Activities," which restructures the U.S. Intelligence Community and provides explicit guidance on all facets of intelligence activities.

1978 A bomb disguised as a package goes off at Northwestern University. This is the first of 16 attacks, over the course of 17 years, by an individual dubbed the "Unabomber" for his principal targets, universities and airlines.

1978 Camp David meetings between U.S. president Carter, Egyptian president Anwar Sadat, and Israeli prime minister Menachem Begin, offer hope for peace in Middle East.

1978 Dissident Georgi Markov is assassinated by an umbrella tip laced with ricin in London by the Bulgarian secret service.

1978 Congress passes the Foreign Intelligence Surveillance Act to regulate electronic intelligence gathering. The act includes the creation of a special court to handle requests by the NSA to perform electronic surveillance on targeted U.S. persons.

1978 Executive Order 12046 establishes National Telecommunications Information Administration to serve as president's advisory on matters involving the radio frequency spectrum.

1978 President Carter, in Executive Order 12065, calls for a review of national security records after 20 years with an eye toward declassification.

1978 DOE initiates its Nuclear Threat Assessment Program at Lawrence Livermore National Laboratory in September.

1978 The U.S. government defines a cipher algorithm for standard use by all government departments, the Digital Encryption Standard.

1978 Kidnapping of Italian former prime minister Aldo Moro; he was seized by the Red Brigade and assassinated 55 days later.

1978 The United States cancels development of the neutron bomb, which would theoretically destroy life but cause minimal physical destruction. The bomb was initially developed, in part, to ensure the maximal survival of European cultural treasures in the advent of nuclear war and thus enhance the credibility of U.S. threats to use the bomb against possible Soviet aggression in western Europe.

1978 The FBI Laboratory Division begins use of laser technology to detect latent crime scene fingerprints.

1979 Egyptian president Sadat and Israeli prime minister Begin sign a peace treaty; other Arab nations protest the treaty.

1979 Congress passes Panama Canal Act. Among its many provisions, the act creates the Panama Canal Commission, which will act as custodian over the canal for the next 20 years.

1979 Sandinistas gain control of Nicaragua.

1979 As a result of a March 28 accident at the Three Mile Island plant outside Harrisburg, Pennsylvania, portions of the reactor's core melts, potentially threatening the health and perhaps even the lives of nearby residents. For several weeks, the nation is gripped by terror as government agencies, including the Nuclear Regulatory Commission, respond to the disaster. No deaths occur as a result of the Three Mile Island accident, but construction of new commercial reactors will be delayed for more than two decades. ARAC and the National Atmospheric Release Advisory Center (NARAC) at Livermore first prove their capabilities by providing DOE and other federal agencies with assessment of the incident.

1979 Use of illegal drugs in the United States reaches its peak, as three out of 10 youth, and one in five adults, reports having used an illegal substance.

1979 President Carter issues an executive order creating the Federal Emergency Management Agency (FEMA).

1979 Saddam Hussein becomes president of Iraq.

1979 The Iranian shah flees Iran, and Shiite Muslim leader Ayatollah Khomeini assumes control of the fundamentalist Islamist revolution. The shah, suffering from cancer, seeks treatment and asylum in the United States. Islamist revolutionaries (mostly Iranian students) seize the American embassy and take 66 Americans hostage. Thirteen hostages are soon released, but the remaining 53 are held until January 20, 1981. The hostage crisis consumes the remainder of U.S. president Carter's term and critics claim that his failure to act decisively to secure the release of the hostages ultimately emboldens a generation of Islamist fundamentalists to commit acts of terrorism against the United States.

1979 Less than a month after the seizure of the U.S. embassy in Tehran, the U.S. embassies in Tripoli, Libya, and Islamabad, Pakistan, are attacked.

1979 Soviets invade Afghanistan on December 24.

1980 CNN, the first 24-hour-a-day cable television news channel, is launched, inspired in part by intense public interest in the Iranian hostage crisis.

1980 After Lech Walesa leads a strike by shipyard workers, Poland's Solidarity Party becomes an independent labor union, the first in the sphere of Soviet influence.

1980 More than five months after the seizure of the U.S. embassy in Tehran, Iran, the United States mounts an attempt to rescue the hostages, but fails when helicopters collide in the desert. The crash forces leaders to abort the mission. Eight Americans die and five are injured in the attempt.

1980 The U.S. Supreme Court rules that a living organism developed by General Electric (a microbe used to clean up an oil spill) can be patented.

1980 Congress passes the Classified Information Procedures Act, which presents guidelines for the use of classified information by both the government and defendants in legal cases.

1980 The United States and 57 other countries boycott the summer Olympics in Moscow to protest Soviet occupation of Afghanistan.

1980 Intelligence Oversight Act replaces the armed services committees with intelligence committees as the principal arm of legislative oversight over the CIA in both houses of Congress.

1980 Iran shells Iraqi border installations at the start of the Iran/Iraq war. Two weeks later, Iraq attacks Iranian air bases.

1980 The Comprehensive Environmental Response, Compensation, and Liability Act (also known as Superfund) is passed in response to the discovery in the late 1970s of a large number of abandoned, leaking hazardous waste dumps. Under Superfund, the Environmental Protection Agency identifies hazardous sites, takes appropriate action, and sees that the responsible party pays for the cleanup.

1980 The Low-Level Radioactive Waste Policy Act is passed, making states responsible for the disposal of their own low-level nuclear waste, such as from hospitals and industry.

1981 AIDS (Acquired Immune Deficiency Syndrome) is recognized and tracked as an epidemic.

1981 Ronald Reagan inaugurated as president of the United States. Fearing Reagan's promise to renew and use American military strength to protect U.S. citizens and interests, Islamist militant revolutionaries in Iran release U.S. hostages held for 444 days.

1981 President Ronald Reagan signs Intelligence Authorization Act of 1981, mandating congressional oversight of covert actions. As part of its oversight of the intelligence community, Congress has passed intelligence authorization acts in every fiscal year since.

1981 President Reagan wounded in assassination attempt by John W. Hinckley, Jr.; three others also wounded.

1981 Israel launches air attacks to destroy an Iraqi nuclear research center at Tuwaythah, Iraq, a city near Baghdad.

1981 In August, two U.S. F-14 Tomcat fighters dispatched by the U.S. Sixth Fleet shoot down two Libyan Su-22 fighter-bombers over the Gulf of Sidra.

1981 Egyptian president Anwar Sadat assassinated by Islamic militants on October 6.

1981 President Reagan reconstitutes the President's Foreign Intelligence Advisory Board and names 19 distinguished citizens outside of government to serve on the Board.

1981 President Reagan signs Executive Order 12333 on December 4, which clarifies ambiguities of previous orders and sets clear goals for the Intelligence Community in accordance with law and regard for the rights of Americans.

1981 Murder of missionaries, December 4: three American nuns and one lay missionary are found murdered outside San Salvador, El Salvador. They are assumed to have been assassinated by a right-wing death squad.

1981 In order to avoid mid-air collisions of increasingly traveled skies, the FAA adopts the aircraft Traffic Alert and Collision Avoidance Systems I and II (TCAS I and II). The system combines radio transmitters and receivers, directional antennas, and computer and cockpit displays to transmit signals called interrogations. Other airplanes in the area receive these signals and transmit replies. Finally, computers calculate the distance between the planes based on time between the interrogation and the reply.

1982 Israel invades Lebanon and ousts PLO forces. In consolidating its occupation of southern Lebanon, which it first invaded in 1978, Israel becomes the first nation to make significant use of unmanned reconnaissance drones in combat.

1982 American journalist James Bamford publishes *The Puzzle Palace,* an expose on the work of the U.S. National Security Agency.

1982 In January, federal law enforcement reorganization gives DEA and FBI concurrent jurisdiction in drug-related criminal matters.

1982 The FDA issues regulations for tamper-resistant packaging after seven people die in Chicago from ingesting Tylenol capsules laced with cyanide. The following year, the federal Anti-Tampering Act is passed, making it a crime to tamper with packaged consumer products.

1982 Spain joins NATO.

1982 With Executive Order 12356, President Reagan bucks the trend of earlier administrations with regard to declassification of national security materials. Reagan tightens the standards with the order, which favors continued classification and even provides conditions for the reclassification of previously declassified documents.

1982 United States withdraws from comprehensive test ban negotiations indefinitely.

1982 President Reagan signs Executive Order 12382, which establishes the National Security Telecommunications Advisory Committee (NSTAC), a presidential advisory board composed of leaders in the telecommunications, finance, and aerospace industries.

1982 U.S. authorities convict four Castro aides of smuggling drugs into the United States, and subsequently uncover a vast Cuban drug-smuggling ring that operates in cooperation with Panamanian leader General Manuel Noriega, as well as with Colombian drug lords.

1982 On June 23, President Reagan signs into law the Intelligence Identities Protection Act, making it a felony to reveal the names of covert intelligence personnel.

1982 In December, Congress passes Boland Amendment to War Powers Act of 1973, forbidding CIA or Department of Defense to support anti-Sandinista forces in Nicaragua.

1983 On January 1, U.S. Defense Department and all participants in its ARPANET officially adopt TCP/IP, a revolutionary new system for network connectivity. Some regard this event as the birth of the Internet.

1983 The Nuclear Waste Policy Act of 1982 is signed, authorizing the development of a high-level nuclear waste repository.

1983 February 13 attack on law enforcement officers in Medina, North Dakota, by the Sheriff's Posse Comitatus is the first significant incident involving an anti-government right-wing terrorist group in the United States.

1983 Bombing of U.S. embassy in Beirut, Lebanon, April 18: sixty-three people, including the CIA's Middle East director, are killed and 120 injured in a 400-pound suicide truck-bomb attack on the U.S. embassy. Islamic Jihad claims responsibility.

1983 Democratic rule is restored in Argentina.

1983 U.S. president Reagan terms the Soviet Union the "evil empire" and announces the Strategic Defense Initiative (Star Wars), a satellite-based defense system that can destroy incoming missiles and warheads in space.

1983 The FBI Hostage Rescue Team becomes fully operational.

1983 In October, President Reagan launches Operation Urgent Fury, the first significant U.S. military action since Vietnam, to overturn a coup on the Caribbean island of Grenada.

1983 Simultaneous suicide truck-bomb attacks on U.S. and French compounds in Beirut, Lebanon. A 12,000-pound bomb destroys the U.S. compound, killing 242 Americans, while 58 French troops are killed when a 400-pound device destroys a French base. Islamic Jihad claims responsibility.

1984 Crime-fighting efforts bolstered by the Sentencing Reform Act, which stiffens prison sentences, requiring mandatory terms for certain crimes and abolishing federal parole; and by the Victims of Crime Act. Throughout the 1980s, numerous national and community-based organizations are formed to provide support to victims of rape, spousal abuse, drunk driving, and other crimes.

1984 Congress enacts legislation making the fraudulent use of credit and debit cards a federal violation.

1984 The Canadian Security and Intelligence Service Act is approved, creating Canadian Security and Intelligence Service.

1984 The DOE, Office of Health and Environmental Research, U.S. Department of Energy (OHER, now Office of Biological and Environmental Research), and the International Commission for Protection Against Environmental Mutagens and Carcinogens (ICPEMC) cosponsor the Alta, Utah, conference highlighting the growing role of recombinant DNA technologies. OTA incorporates the proceedings of the meeting into a report acknowledging the value of deciphering the human genome.

1984 President Reagan issues a directive giving the NSA responsibility of maintaining security of government computers.

1984 DOE Office of Security establishes Central Training Academy. Now known as Nonproliferation and National Security Institute, this facility provides training in counterintelligence and other areas to more than 100 government departments and agencies.

1984 Islamic Jihad kidnaps and later murders CIA station chief William Buckley in Beirut, Lebanon. Other U.S. citizens not connected to the U.S. government are subsequently seized over a two-year period.

1984 With Executive Order 12472, signed on April 3, President Reagan expands the mission of the National Communications System.

1984 Strategic Defense Initiative Organization (SDIO) chartered in April by secretary of defense Caspar Weinberger.

1984 CIA Information Act, signed by President Reagan on October 15, exempts the agency from the search and review requirements of the Freedom of Information Act.

1984 Eighteen U.S. servicemen are killed and 83 people are injured in a bomb attack on a restaurant near a

U.S. air force base in Spain. Hezbollah claims responsibility.

1984 Sikh terrorists seize the Golden Temple in Amritsar, India. One hundred people die as Indian security forces retake the Sikh holy shrine.

1984 Assassination of Indian prime minister Indira Gandhi, October 31; she is shot to death by members of her security force.

1985 Mikhail Gorbachev becomes general secretary of the Communist Party in the Soviet Union. Gorbachev institutes economic reforms and policies such as ''glasnost'' (openness) to ease Cold War tensions.

1985 Called "the year of the spy," 1985 features a series of high-profile espionage cases and arrests. In May, the John Walker Spy Ring is arrested. Former navy personnel John Walker, Jerry Whitworth, Arthur Walker, and Michael Walker are convicted of or plead guilty to passing classified material to the Soviet Union. On November 21, Jonathan Jay Pollard, a navy intelligence analyst, is arrested for spying for Israel. On November 23, Larry Wu Tai Chin, a former CIA analyst, is arrested on charges of spying for the People's Republic of China since 1952. On November 25, a third major spy, former National Security Agency employee William Pelton, is arrested and charged with selling military secrets to the Soviets.

1985 Alec Jeffreys develops "genetic fingerprinting," a method of using DNA polymorphisms (unique sequences of DNA) to identify individuals. The method, which is subsequently used in paternity, immigration, and murder cases, is generally referred to as "DNA fingerprinting."

1985 David Deutsch advances theory of quantum computing.

1985 Kary Mullis, working at Cetus Corporation, develops the polymerase chain reaction (PCR), a new method of amplifying DNA. This technique quickly becomes one of the most powerful tools of molecular biology. Cetus patents PCR and sells the patent to Hoffman-LaRoche, Inc. in 1991.

1985 The Global Positioning System (GPS) becomes operational.

1985 U.S. air force and army join forces to develop the J-STARS (Joint Surveillance and Target Acquisition Radar System) aircraft.

1985 Federal Radiological Preparedness Coordinating Committee, appointed by the Federal Emergency Management Agency (FEMA), completes the U.S. Federal Radiological Emergency Response Plan, a blueprint for the federal response to a hazard involving nuclear radiation.

1985 TWA hijacking, June 14: A Trans-World Airlines flight is hijacked en route to Rome from Athens by two Lebanese Hezbollah terrorists and forced to fly to Beirut. The eight crew members and 145 passengers are held for 17 days, during which one American hostage, a U.S. sailor, is murdered. After being flown twice to Algiers, the aircraft is returned to Beirut after Israel released 435 Lebanese and Palestinian prisoners.

1985 *Achille Lauro* hijacking, October 7: Four Palestinian Liberation Front terrorists seize an Italian cruise ship in the eastern Mediterranean Sea, taking more than 700 hostages. One elderly U.S. passenger is murdered.

1985 The Soviet Union announces a nuclear testing moratorium.

1986 The space shuttle *Challenger* explodes shortly after lift-off. Gaskets weakened by unusually cold weather are blamed for the accident, which leads to intense scrutiny of NASA safety procedures.

1986 Explosion at the Chernobyl nuclear plant in the Ukraine causes severe radiation leakage and an estimated 8,000 near-term deaths.

1986 U.S. sales of arms to Iran during its war with Iraq and the use of profits to fund anti-government, or Contra, forces in Nicaragua fuels the Iran-Contra scandal.

1986 DNA analysis conducted by the Scientific Intelligence Unit of England's Scotland Yard leads to the first conviction of a criminal—Colin Pitchfork, accused of rape and murder—on the basis of DNA evidence.

1986 Tension escalates between the United States and Libya in the Gulf of Sidra, off the coast of Libya, as U.S. and Libyan forces skirmish. The conflict culminates on April 15 in devastating U.S. air strikes on targets within Libya.

1986 Congress passes Anti-Drug Abuse Act. This federal law includes mandatory minimum sentences for first time offenders with harsher penalties for possession of crack cocaine than powder cocaine.

1986 Computer Fraud and Abuse Act is enacted, defining federal computer crimes.

1986 U.S. intelligence community establishes Intelligence Community Staff Committee on MASINT (measurement and signatures intelligence) to oversee all relevant activities.

1986 Congress passes Emergency Planning and Community Right-to-Know Act (EPCRA), which establishes guidelines whereby federal agencies assist local communities in the event of a toxic chemical spill or related incident.

1986 U.S. Defense Department establishes Chemical and Biological Defense Analysis Center.

1986 Congress passes Goldwater-Nichols Act, the fourth major reorganization of the U.S. Department of Defense since World War II. The act calls on the White House to issue an annual National Security Strategy.

1986 United States Congress passes the Electronic Communication Privacy Act.

1986 Clayton Lonetree, the only U.S. Marine convicted of espionage, turns himself in to the CIA.

1987 Congress passes the Computer Security Act, which makes unclassified computing systems the responsibility of the National Institute of Standards and Technology (NIST) and not the NSA with regard to technology standards development.

1987 Iraqi government uses nerve agents including sarin against Kurds in Northern Iraq.

1987 Founding of U.S. Special Operations Command, which brings together special operations forces from the army, navy, and air force.

1987 The PLO's terrorist campaign against Israel becomes acute during its first Intifada (or "shaking off") of Israeli authority in the occupied territories.

1987 North Korean agents plant a bomb that destroys Korean Air Lines Flight 858.

1987 Nuclear Waste Policy Amendments Act designates Yucca Mountain, Nevada, as candidate site for the nation's first geological repository for high-level radioactive waste.

1987 Soviet president Gorbachev and U.S. president Reagan sign the Intermediate-Range Nuclear Forces (INF) Treaty.

1987 The idea to use patterns of the iris of the eye as an identification marker is patented, along with the algorithms necessary for iris identification.

1988 U.S. Marine Corps Lt. Col. W. Higgins is kidnapped and murdered by the Iranian-backed Hezbollah group while serving with the UN Truce Supervisory Organization (UNTSO) in Lebanon.

1988 Congress passes the Prescription Drug Marketing Act designed to maintain the sale and distribution of prescription drugs through legitimate commercial channels. The new law requires state-level licensing for drug wholesalers, restricts drug reimportation from other countries, institutes regulations regarding drug samples, and prohibits the traffic or counterfeiting of redeemable drug coupons.

1988 The Food and Drug Administration Act officially establishes the FDA as an agency of the Department of Health and Human Services. The act provides for a Commissioner of Food and Drugs appointed by the president and outlines the responsibilities of the secretary and the commissioner for research, enforcement, education, and information.

1988 The Human Genome Organization (HUGO) is established by scientists in order to coordinate international efforts to sequence the human genome.

1988 First test flight of J-STARS (Joint Surveillance and Target Acquisition Radar System) aircraft.

1988 Congress passes National Defense Authorization Act, establishing the Defense Nuclear Facilities Safety Board as an independent agency charged with overseeing the disposition of defensive nuclear materials.

1988 Iran-Iraq ceasefire begins, monitored by the UN Iran-Iraq Military Observer Group (UNIIMOG).

1988 The federal Polygraph Protection Act prohibits employers from using polygraphs for employment screening.

1988 Libyan intelligence operatives plant a bomb aboard Pan-Am flight 103, which crashes into the village of Lockerbie, Scotland, killing all 259 aboard and 11 persons on the ground. Two Libyan intelligence officers are ultimately tried under Scottish law in The Hague. One of them, Abdelbaset Ali Mohmed Al Megrahi, is found guilty in January 2001; the other, Al Amin Khalifa Fhimah, is acquitted.

1989 After nine years of war, Soviet forces withdraw from Afghanistan.

1989 British Parliament passes Security Service Act, which for the first time confers legal status on MI5.

1989 Charles H. Bennett and Gilles Brassard develop first quantum computer.

1989 United States signs Berne Convention for the Protection of Literary and Artistic Works.

1989 The New People's Army (NPA) assassinates U.S. army colonel James Rowe in Manila in April. The NPA also assassinates two U.S. government defense contractors in September.

1989 The Berlin Wall is torn down, as many communist governments in Eastern Europe collapse.

1989 In December, U.S. forces attack Panama to remove General Manuel Noriega in Operation Just Cause. The U.S. army uses loud music as part of a psychological operation to dislodge Noriega from his refuge at the Vatican embassy.

1989 Nicolae Ceausescu, communist dictator of Romania, is overthrown and executed.

1990 Yugoslavia overthrows Communist Party and ethnic tensions mount.

1990 U.S. embassy in Peru bombed by the Tupac Amaru Revolutionary Movement.

1990 Syrian troops intervene in Lebanon's civil war.

1990 Iraq invades Kuwait. UN Security Council passes resolution 660 calling for full Iraqi withdrawal. President George H.W. Bush vows "this aggression will not stand" and launches Operation Desert Shield, a buildup of U.S. forces in the region in preparation for a possible armed confrontation.

1990 U.S. military personnel receive vaccinations against anthrax prior to duty in the Persian Gulf.

1990 UN, via resolution 661, imposes economic sanctions on Iraq.

1990 East and West Germany reunited.

1990 Former Solidarity union leader Lech Walesa becomes president of post-communist Poland.

1990 NATO and Warsaw Pact nations sign Conventional Armed Forces in Europe treaty (CFE), which promises mutual non-aggression.

1990 U.S. Strategic Air Command brings to an end the 24-hour-a-day operation of its Airborne Command Post, Looking Glass, on July 24.

1990 Iraq hangs Farzad Bazoft, an Iranian-born journalist with the *London Observer* newspaper, whom Hussein accuses of spying on Iraqi military installations.

1990 Space shuttle *Atlantis* completes secret mission to place a spy satellite in orbit.

1991 First-ever use of the strategic petroleum reserve to stabilize world oil prices following the Iraqi invasion of Kuwait.

1991 Launch of Operation Desert Storm against Iraq on January 17. The initial bombing campaign lasts approximately 100 hours, and the entire military operation takes only 42 days. The result is overwhelming Iraqi defeat.

1991 Carbon-graphite coils capable of generating an electromagnetic pulse or otherwise disabling electronics are used in U.S.-led raids on Baghdad, Iraq.

1991 J-STARS aircraft gain their first combat experience in Operation Desert Storm.

1991 Saddam Hussein orders Iraqi forces to brutally suppress Kurd and Shia rebellions in northern and southern Iraq.

1991 IAEA's Iraq Action Team begins inspecting suspect sites in Iraq under UN Security Council mandate. UN also establishes a safe-haven in northern Iraq, north of latitude 36 degrees north, for the protection of the Kurds. Subsequently, the United States orders Iraq to end all military activity and establishes north and south "no-fly" zones.

1991 Soviet president Mikhail Gorbachev announces that the Soviet Union will unilaterally cease nuclear testing for one year.

1991 The United States and Soviet Union sign historic agreement to cut back long-range nuclear weapons by more than 30 percent over the next seven years.

1991 The Warsaw Pact is officially dissolved.

1991 The Baltic republics—Latvia, Lithuania, and Estonia—declare their independence and the Soviet Union crumbles. A commonwealth of independent states takes the place of the former Soviet empire. Boris Yeltsin becomes president of Russia.

1991 U.S. Navy Fleet Intelligence Center (FIC) Pacific (FICPAC) and FIC Europe-Atlantic (FICEURLANT) absorbed into National Military Joint Intelligence Center (NMJIC).

1991 U.S. Army Intelligence Agency ceases to exist; absorbed by Intelligence and Security Command (INSCOM).

1991 Lustration law enacted in the Czech Republic, barring persons who had collaborated with the secret police during communist rule from serving in most public posts.

1991 In December, Britain's MI5 signals a new era of openness when it announces the appointment of a new director-general, Stella Rimington, the first MI5 chief to be publicly identified.

1992 Federal Republic of Yugoslavia collapses; fierce fighting between ethnic groups ensues.

1992 The U.S. Army begins collecting blood and tissue samples from all new recruits as part of a "genetic dog tag" program aimed at better identification of soldiers killed in combat.

1992 Naval Criminal Investigative Service formed as an entity separate from the Office of Naval Intelligence.

1992 In August, DEA creates its Intelligence Division.

1992 Land Remote Sensing Policy Act of 1992 establishes legal basis for ownership and operation of commercial remote sensing satellites in the United States.

1992 The FBI establishes a Criminal Justice Information Services (CJIS) Division.

1992 The United States conducts its last nuclear explosion test in September.

1993 Czechoslovakia dissolves into the Czech Republic and Slovakia.

1993 The Maastricht Treaty officially forms the European Union.

1993 U.S. Congress passes the Domestic Chemical Diversion Control Act, aimed to stop the conversion of legal substances into illegal substances.

1993 February 26: the World Trade Center in New York City is badly damaged when a car bomb planted by Islamic terrorists explodes in an underground garage. The bombing leaves six people dead and 1,000 injured. The men carrying out the attack were followers of Umar Abd al-Rahman, an Islamic cleric who preached in the New York City area.

1993 After a 51-day siege by the Bureau of Alcohol, Tobacco, and Firearms, federal teams assault a compound held by the Branch Davidians, a religious sect charged with hoarding illegal weapons. The Branch Davidians set the buildings on fire, killing 76 people, including cult leader David Koresh.

1993 On April 14, Iraqi intelligence agents attempt to assassinate former president George H.W. Bush during a visit to Kuwait. Two months later, President William J. Clinton launches a cruise missile attack on the Iraqi capital of Baghdad.

1993 U.S. Department of Defense closes the Naval Intelligence Command, whose functions—along with those of the Naval Technical Intelligence Center, Task Force 168, and the Navy Operational Intelligence Center—are absorbed by the Office of Naval Intelligence.

1993 China defies informal global moratorium on nuclear testing with a weapons test.

1993 The final Global Positioning Satellite (GPS) is placed into orbit and the GPS system becomes fully operational.

1993 Explosive growth of Internet begins as a result of two factors: the full opening of the National Science Foundation's NSFNET, and the development of the first browsers, Mosaic (forerunner of Netscape Navigator) and Microsoft Internet Explorer.

1993 In October, U.S. Air Force Air Intelligence Agency replaces Air Force Intelligence Service.

1993 On October 3, 18 U.S. Rangers, participants in a UN peacekeeping force in Somalia, are killed in a firefight on the streets of Mogadishu.

1993 In the wake of a congressional ban on the deployment of space-based weapons, the Ballistic Missile

Defense Organization (BMDO) forms. The collapse of the former Soviet Union makes a large-scale attack upon the United States appear much less likely and Congress seeks to push the DOD to update missile defense programs to address the dangers of the post-Cold War world. In this changed political climate, secretary of defense Les Aspin announces that former president Reagan's ten-year-old Strategic Defense Initiative (popularly known as "Star Wars") will be terminated, with missile defense responsibilities transferred to the newly formed BMDO.

1993 *Time* magazine names the personal computer as its "man of the year," as personal computer sales skyrocket, changing the way people around the world work, play and communicate.

1994 The Genetic Privacy Act, the first U.S. Human Genome Project legislative product, proposes regulation of the collection, analysis, storage, and use of DNA samples and genetic information. These rules were endorsed by the ELSI Working Group.

1994 Aldrich Ames, a 30-year CIA veteran, and his wife, Maria del Rosario Casas Ames, are arrested on espionage charges for selling secrets to the former Soviet Union.

1994 Jewish right-wing extremist and U.S. citizen Baruch Goldstein kills Muslim worshippers at a mosque in the West Bank town of Hebron, killing 29 and wounding about 150.

1994 North Korea withdraws its membership from IAEA over dispute regarding nuclear inspections.

1994 U.S. Navy, Marine, and Coast Guard intelligence agencies begin operating jointly from the National Maritime Intelligence Center in Suitland, Maryland.

1994 Congress reduces the lifetime-protection provisions for U.S. presidents, authorizing Secret Service protection only for the first 10 years after leaving office. The new law applies to all presidents in office after January 1, 1997.

1994 Britain's Parliament passes Intelligence Services Act, which gives MI6 new statutory grounding. The Act defines the responsibilities and functions of MI6 and its chief, and sets in place a framework of government oversight for MI6 activities.

1994 U.S. military action in Haiti restores government of ousted president Jean-Bertrand Aristide.

1994 After Rwandan dictator Major General Juvenal Habyarimana dies in a plane crash on April 6, his Hutu supporters blame the Tutsi-controlled Rwandan Patriotic Front, and launch a campaign of genocide that results in more than 800,000 deaths.

1994 Russia invades Chechnya on October 11, launching a war that will last almost two years.

1995 Combinatorial chemistry, a technique which quickly surveys huge numbers of chemical combinations in order to select the most desirable molecular configurations, attracts the attentions of chemical companies. Scientists predict the possibility of creating numerous new chemicals to serve the needs of industrial and pharmaceutical development, along with defense technology.

1995 President Clinton signs Executive Order 12968 on February 22, which provides rules for access to classified information.

1995 Study by the Rand Corporation finds that every dollar spent in drug treatment saves society seven dollars in crime, policing, incarceration, and health services.

1995 UN Security Council resolution 986 allows partial resumption of Iraqi oil exports, with the original intent to allow Iraq to sell oil to buy food and medicine (the "oil-for-food program"). Iraq subsequently diverts funds from sales to additional weapons purchases and the building of offices and places for the Hussein government. Malnutrition and improper medical care becomes widespread in Iraq.

1995 After thwarting UN weapons inspectors, the government of Iraq admits to producing over 8,000 liters of concentrated anthrax as part of the nation's biological weapons program.

1995 Twelve are killed and 5,700 injured in a sarin nerve gas attack on a crowded subway station in the center of Tokyo. Aum Shinri-kyu cult is blamed for the attacks.

1995 A truck bomb explodes outside the Alfred P. Murrah Federal office building in Oklahoma City, Oklahoma, on April 19, collapsing walls and floors. The massive explosion kills 169, including 19 children and one person who dies in the rescue effort. Timothy McVeigh and Terry Nichols are later convicted in the anti-government plot to avenge the Branch Davidian standoff in Waco, Texas, exactly two years earlier.

1995 Concerned by revelations that agents of the CIA have committed human rights violations in Guatemala, the CIA draws up guidelines prohibiting the agency from hiring agents with records of human-rights violations.

1995 June 1995, while Comprehensive Nuclear Test Ban Treaty (CTBT) negotiations are still under way, France announces that it will resume nuclear testing.

1995 President Clinton issues Presidential Decision Directive 39, "U.S. Policy on Counterterrorism," calling for a number of specific efforts to deter terrorism in the U.S. as well as attacks on its citizens and allies abroad.

1995 Radical Sunni Muslims set off a bomb at a national guard facility in Riyadh, Saudi Arabia, killing five Americans.

1995 NATO launches air strikes against Bosnian Serb positions to force the Bosnian Serbs to negotiate a peace settlement. NATO deploys Implementation Force (Ifor) to monitor and enforce a ceasefire.

1995 Dayton Accords end fighting in Bosnia.

1996 Defense Authorization Act directs Advanced Research Projects Agency (ARPA) to once again be named the Defense Advanced Research Projects Agency (DARPA).

1996 An Irish Republican Army (IRA) bomb detonates in London on February 9, killing two persons and wounding more than 100 others, including two U.S. citizens.

1996 International participants in the genome project meet in Bermuda and agree to formalize the conditions of

data access. The agreement, known as the "Bermuda Principles," calls for the release of sequence data into public databases within 24 hours.

1996 National Imagery and Mapping Agency (NIMA) created by the consolidation of several existing government and military agencies.

1996 The Health Care Portability and Accountability Act incorporates provisions to prohibit the use of genetic information in certain health-insurance eligibility decisions. The Department of Health and Human Services is charged with the enforcement of health-information privacy provisions.

1996 U.S. signs the Comprehensive Test Ban Treaty, but the Senate ultimately refuses (in 1999) to ratify the treaty.

1996 In an effort to reduce counterfeiting, federal government makes first major change to U.S. currency in 70 years.

1996 The Chemical and Biological Incident Response Force (CBIRF), a unit of the U.S. Marines devoted to countering chemical or biological threats at home and abroad, is activated.

1996 World chess champion Garry Kasparov, able to compute the ramifications of 2–3 chess moves per second, loses a chess match to IBM's Deep Blue computer, able to compute the ramifications of 200 million moves per second.

1996 France conducts its last nuclear weapons test and immediately afterwards French president Jacques Chirac announces his support for a comprehensive test ban.

1996 A fuel truck carrying a bomb explodes outside the U.S. military's Khobar Towers housing facility in Dhahran, Saudi Arabia, on June 25, killing 19 U.S. military personnel and wounding 515 persons, including 240 U.S. personnel. Thirteen Saudis and a Lebanese, all alleged members of Islamic militant group Hezbollah, are eventually indicted.

1996 China conducts its last nuclear explosion test.

1996 Bombing at Atlanta's Centennial Olympic Park on July 27, during the Olympic Games, kills two people and injures 112. Eric Robert Rudolph is charged with the crime, but he evades the authorities until his capture in 2003.

1996 Dolphins and sea lions used to protect waters off San Diego during the Republican Party convention.

1996 On October 11, President Clinton signs into law the Economic Espionage Act, which makes it a federal crime to use unauthorized means to obtain any trade secret whose transfer to other parties would cause economic harm to its lawful owner.

1996 Twenty-three members of the Tupac Amaru Revolutionary Movement (MRTA) take several hundred people hostage at a party given at the Japanese Ambassador's residence in Lima, Peru on December 17. Among the hostages were several U.S. officials, foreign ambassadors and other diplomats, Peruvian Government officials, and Japanese businessmen. The group demanded the release of all MRTA members in prison and safe passage for them and the hostage takers. The terrorists released most of the hostages in December but held 81 Peruvians and Japanese citizens for several months.

1996 U.S. Economic Espionage Act passed.

1997 Ian Wilmut of the Roslin Institute in Edinburgh, Scotland, announces the birth of a lamb called Dolly, the first mammal cloned from an adult cell, specifically, a cell in a pregnant ewe's mammary gland.

1997 The National Center for Human Genome Research (NCHGR) at the National Institutes of Health becomes the National Human Genome Research Institute (NHGRI).

1997 U.S. National Cancer Institute estimates that 160 million people in the United States were exposed to some level of iodine 131 from prior U.S. nuclear tests conducted in Nevada, and that these exposures would, over time, cause 30,000–75,000 cases of thyroid cancer.

1997 Congress passes the Fair Credit Reporting Act (FCRA), which establishes rights involving records from consumer reporting agencies.

1997 Department of Energy creates Chemical and Biological National Security Program to develop systems and technologies to protect civilian populations against the threats associated with chemical, biological, and nuclear attacks.

1997 The corrupt regime of Mobutu Sese Seko, a longtime U.S. ally in Zaire, is overthrown by rebel forces under the leadership of Laurent Kabila. Kabila will change the country's name back to Congo, but his regime will bring few democratic reforms, and he will be killed by his own bodyguards in 2001.

1997 Tourist killings in Egypt, November 17. Al-Gama'at al-Islamiyya (IG) gunmen shoot and kill 58 tourists and four Egyptians and wound 26 others at the Hatshepsut Temple in the Valley of the Kings near Luxor.

1997 The FBI announces its new National DNA Index System (NDIS) on December 8, allowing forensic science laboratories to link serial violent crimes to each other and to known sex offenders through the electronic exchange of DNA profiles.

1998 The Hebron Accord, designed to promote peace between Israel and Palestine, is undermined by both sides as terrorism breaks out and the building of new settlements defies non-expansionist agreements.

1998 Craig Venter forms a company (later named Celera), and predicts that the company will decode the entire human genome within three years. Celera plans to use a "whole genome shotgun" method, which will assemble the genome without using maps. Venter says that his company will not follow the Bermuda principles concerning data release.

1998 DNA analyses of semen stains on a dress worn by White House aide Monica Lewinsky are found to match DNA from a blood sample taken from President Clinton.

1998 DNA fingerprinting used to identify remains of Russian Imperial Romanov family.

1998 India and Pakistan conduct underground nuclear tests. Exaggerated results are detected using seismic records.

1998 Controversy breaks out over the reported NSA Echelon project, which privacy groups describe as a worldwide surveillance network that eavesdrops on communications traffic and shares intelligence gathered by the United States, Great Britain, Canada, Australia and New Zealand.

1998 International Atomic Energy Agency Iraq Action Team withdraws from Iraq because of a lack of "full and free access" to Iraqi sites.

1998 Congress passes Digital Millennium Copyright Act (DMCA), the most comprehensive overhaul of copyright law in a generation.

1998 Presidential Decision Directive 61, issued by President Clinton in February, reorganizes DOE Office of Intelligence.

1998 U.S. Army combines its Chemical and Biological Defense Command and Soldier Systems Command to form U.S. Army Soldier and Biological Chemical Command (SBCCOM).

1998 Due to heightened concerns over technology leaks from the U.S. Commerce Department to China, commerce secretary William Daley announces plans to tighten security and limit access to classified information within the department.

1998 Presidential Decision Directive 63, signed by President Clinton in May, establishes the Critical Infrastructure Assurance Office (CIAO) of the U.S. Department of Commerce.

1998 Real IRA explodes a car bomb outside a store in Banbridge, Northern Ireland.

1998 U.S. embassy bombings in East Africa, August 7, 1998: A bomb explodes at the rear entrance of the U.S. embassy in Nairobi, Kenya, killing 12 U.S. citizens, 32 foreign service workers, and 247 Kenyan citizens. About 5,000 Kenyans, six U.S. citizens, and 13 foreign service workers are injured. Almost simultaneously, a bomb detonates outside the U.S. embassy in Dar es Salaam, Tanzania, killing seven foreign service workers and three Tanzanian citizens, and injuring one U.S. citizen and 76 Tanzanians. The U.S. government holds Osama Bin Laden responsible.

1998 Formation, in October, of the U.S. National Domestic Preparedness Office as the coordination center for all federal efforts in response to weapons of mass destruction.

1998 Digital Millennium Copyright Act (DMCA) passed.

1998 Iraq expels UN weapons inspectors on October 31. In December, the United States and Britain launch Operation Desert Fox to attempt to destroy Iraq's nuclear, chemical, and biological weapons programs.

1999 Vladimir Putin becomes prime minister of Russia.

1999 The Czech Republic, Hungary, and Poland become the first former Soviet bloc states to join NATO, taking the alliance's borders some 400 miles towards Russia.

1999 President Clinton signs Executive Order 13142, which amends Executive Order 12958 by extending the period of classification for some sensitive documents.

1999 Taiwanese-born computer scientist Wen Ho Lee is fired from his job in March and subsequently arrested by the FBI. Charged with not properly securing classified materials and failing to report meetings with individuals from "sensitive" countries, Lee will be held for a year and eventually convicted in 2000.

1999 Beginning March 24, NATO forces conduct a 78-day campaign of air strikes to end Serb "ethnic cleansing" in the Albanian enclave of Kosovo and to break the hold of Serbian leader Slobodan Milosevic.

1999 Melissa virus (actually a form of malicious data wedded to a particular type of virus program, a macro virus) spreads through the e-mail systems of the world on March 26, causing $80 million worth of damage, primarily in the form of lost productivity resulting from the shutdown of overloaded mailboxes.

1999 Osama bin Laden is added to the FBI's Ten Most Wanted Fugitives list in June, in connection with the U.S. embassy bombings in eastern Africa.

1999 FBI personnel travel to Kosovo on June 23 to assist in the collection of evidence and the examination of forensic materials in support of the prosecution of Slobodan Milosevic and others before the International Criminal Tribunal for the former Yugoslavia.

1999 Congress releases a bipartisan report asserting that China stole nuclear secrets regarding U.S. weapons. The systematic espionage campaign by the Chinese is alleged to date to the 1970s.

1999 A nuclear accident at Japan's Tokaimura facility occurs on September 30 when a criticality event, or unplanned chain reaction, exposes 39 workers to radiation contamination and causes the evacuation of families within 350 meters of the facility.

1999 Russia invades Chechnya on October 1, resuming hostilities that had abated since 1996.

1999 IKONOS, the world's first commercial remote sensing satellite with 1 meter resolution, is launched.

1999 UN Security Council resolution 1284 creates the UN Monitoring, Verification and Inspection Commission (UNMOVIC) as a replacement for UNSCOM. Saddam Hussein rejects the resolution. In March 2000, Hans Blix becomes chairman of UNMOVIC.

1999 A merger of the ACDA and U.S. State Department creates a number of new bureaus, including the Bureau of Arms Control.

1999 As the year 2000 approaches, the world prepares itself for the possible deleterious effects of a computer shortcut (a protocol developed when memory was scarce) that used only the last two digits of a year to indicate the year. Termed the Y2K problem, fears approach near hysteria as people and governments prepare for computers to malfunction and adversely effect critical infrastructure. Adequate preparation, considerable investment in programming solutions,

and monitoring turn the dawn of 2000 into a grand worldwide party but a non-event with regard to Y2K fears. Minimal disruptions are reported.

2000 Mokhtar Haouari and Abdel Ghani Meskini are charged with collaborating with Ahmed Ressam and others in a wide-ranging terrorist conspiracy to bomb U.S. sites during the January 1, 2000, millennium celebrations. The FBI/New York Police Department Joint Terrorist Task Force, Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, and Canada's Department of Justice collaborate in the investigation.

2000 Islamic extremist group Asbat al-Ansar carries out a rocket-propelled grenade attack on the Russian embassy in Beirut in January 2000.

2000 The Jaish-e-Mohammed, an Islamic extremist group based in Pakistan, is formed by Masood Azhar upon his release from prison in India in early 2000.

2000 President Clinton signs an executive order prohibiting federal departments and agencies from using genetic information in hiring or promoting workers.

2000 NNSA begins operations on March 1, 2000. NNSA has the mission of improving national security through defense uses of nuclear energy.

2000 Beginning in October, OIS divides its functions between its Information Security Services Center and its new Office of Information Assurance and Critical Infrastructure Protection.

2000 October 12, terrorist bombing of USS *Cole* kills 17 of its crew and wounds 39 others. Two suicide bombers, ultimately linked to al-Qaeda, pull alongside the vessel near the port in Aden, Yemen, and detonate explosives near the *Cole*'s hull.

2000 The PLO's terrorist campaign against Israel again intensifies with start of a second Intifada.

2000 Former U.S. senator John Danforth, conducting an independent review of FBI actions in the 1993 FBI assault on the Branch Davidian compound in Waco, Texas, releases his final report exonerating the FBI of wrongdoing. The Government Operations Committee reaches a similar conclusion.

2001 On January 5, just 15 days before leaving office, President Clinton issues Presidential Decision Directive (PDD) 75, "U.S. Counterintelligence Effectiveness—Counterintelligence for the Twenty-first Century."

2001 A U.S. Navy P-3 on a surveillance mission over the South China Sea collides with a Chinese fighter plane, killing the Chinese pilot and forcing the American plane to make an emergency landing on China's Hainan Island. Although the Chinese pilot is blamed for the collision, Washington issues "regrets" but no apology (as is demanded by the Chinese) to secure the release of the U.S. crew after they are held for 11 days.

2001 The FBI announces on January 5 the National InfraGuard program at the FBI's National Infrastructure Protection Center. The program centers on securely sharing information about computer intrusions and intrusion threats between business and law enforcement so that the confidentiality of potentially affected businesses is protected.

2001 The complete draft sequence of the human genome is published in February. The public sequence data is published in the British journal *Nature* and the Celera sequence is published in the American journal *Science.* Increased knowledge of the human genome allows greater specificity in pharmacological research and drug interaction studies.

2001 FBI Agent Robert Philip Hanssen is arrested on February 18 for conspiracy to commit espionage. The affidavit in support of an arrest warrant for Hanssen charges that he engaged in a lengthy relationship with the KGB and its agencies.

2001 Following years of Iraqi firings upon U.S. and British airplanes patrolling the northern and southern "no fly" zones, the United States and Britain carry out bombing raids in February with the intent to disable Iraq's air defense network.

2001 President George W. Bush presents the Congressional Gold Medal to World War II Navajo code talkers (windtalkers).

2001 In May, Libyan leader Muammar Qaddafi admits to a German newspaper that Libya was behind a Berlin discotheque bombing in 1986 that killed a U.S. serviceman and a Turkish civilian, and injured some 200 others. At a trial in November, four defendants are convicted for roles in the bombing.

2001 Hamas claims responsibility for the bombing of a popular Israeli nightclub that causes more than 140 casualties.

2001 A U.S. grand jury indicts fourteen Hezbollah members on June 21 for the 1996 Khobar Towers bombing.

2001 Ahmad Shah Massoud, the leader of the rebels in the Afghanistan Northern Alliance, widely regarded as the most popular opposition figure to the ruling Taliban (the regime providing asylum to al-Qaeda and its leader, Osama bin Laden) is assassinated on September 9.

2001 September 11, Islamist terrorists mount coordinated attacks on New York and Washington. The World Trade Center towers are destroyed, killing nearly 3,000 people. In Washington, a plane slams into the Pentagon, while passengers aboard another hijacked airliner, aware of the other terrorist attacks, fight back. During the struggle for the aircraft, it crashes into a Pennsylvania field, thwarting the terrorists' plans to crash the plane into either the U.S. Capitol or the White House. The FBI dedicates 7,000 of its 11,000 special agents and thousands of FBI support personnel to the PENTTBOM investigation. "PENTTBOM" is short for Pentagon, Twin Towers Bombing.

2001 Letters containing a powdered form of *Bacillus anthracis*, the bacteria that causes anthrax, are mailed by an unknown terrorist or terrorist group (foreign or domestic) to government representatives, members of the news media, and others in the United States. More than 20 cases and five deaths are eventually attributed to the terrorist attack.

2001 On October 7, United States launches Operation Enduring Freedom against the al-Qaeda terror network and Afghanistan's Taliban regime. The Taliban regime is toppled and many al-Qaeda operatives are killed, but Osama bin Laden evades capture.

2001 Following the September 11 attacks, NATO secretary-general George Robertson invokes Article Five of the alliance's constitution, which states that an attack on one member nation is seen as an attack on all. Washington chooses, however, not to involve NATO in the U.S.-led military campaign which follows.

2001 QuickBird satellite launched, providing sub meter commercial satellite images.

2001 On October 16, President Bush signs Executive Order 13231, "Critical Infrastructure Protection in the Information Age."

2001 On October 26, President Bush signs the USA Patriot Act into law, giving the FBI and CIA broader investigatory powers and allowing them to share confidential information about suspected terrorists with one another. Under the act, both agencies can conduct residential searches without a warrant and without the presence of the suspect and immediately seize personal records. The provisions are not limited to investigating suspected terrorists, but may be used in any criminal investigation related to terrorism. The Patriot Act also grants the FBI and CIA greater latitude in using computer tracking devices such as the Carnivore (DCS1000) to gain access to Internet and phone records.

2001 Disarmament operations begin in the former Yugoslav republic of Macedonia.

2001 Chernobyl nuclear power plant begins decommissioning.

2001 In *United States v. Scarfo,* a federal judge in Newark, New Jersey, grants the government's motion to suppress information on an FBI computer keystroke recording device under the Classified Information Protection Act (CIPA).

2001 Fourth Marine Expeditionary Brigade formed. It consists of the Marine Security Force Battalion, the Marine Security Guard Battalion, the Chemical and Biological Incident Response Force, and the new anti-terrorism battalion. The latter had evolved from the 1st Battalion, 8th Marines, which had been hit in the 1983 bombings of U.S. Marine barracks in Lebanon.

2001 On November 19, President George W. Bush signs into law the Aviation and Transportation Security Act (ATSA), which creates the Transportation Security Administration (TSA), and authorizes TSA to direct a team of air marshals and federal airport security screeners.

2001 United Kingdom passes a new counter-terrorist bill in December, the Anti-Terrorism, Crime, and Security Act. The act allows British authorities to detain suspected terrorists for up to six months before reviewing their cases and for additional six-month periods after that. As in the United States, civil liberty advocate groups in the United Kingdom criticize the new law for potentially infringing upon a basic civil liberty, specifically the right to avoid unlawful detention and gain access to a speedy trial.

2001 The Chemical and Biological Incident Response Force (CBIRF) sends a 100-member initial response team into the Dirksen Senate Office Building in Washington on December 2 alongside EPA specialists to detect and remove anthrax spores which had been introduced into the building in a letter. A similar mission was undertaken at the Longworth House Office Building in October, during which time samples were collected from more than 200 office spaces.

2001 FBI Director Mueller orders the reorganization of FBI operations on December 3 to respond to a revised agency mission that emphasizes terrorism prevention and internal accountability, and strengthens partnerships with domestic and international law enforcement.

2001 Enough closed-circuit television cameras (CCTV) are installed in public places in Britain that, on an average day in any large British city, security experts calculate that a person will have over 300 opportunities to be captured on CCTV during the course of normal daily activities.

2001 U.S. unmanned plane completes trans-Pacific flight from California to Australia.

2001 Brian Regan, retired U.S. Air Force master sergeant and cryptanalyst, is arrested on charges of spying for Iraq, Libya and China.

2002 In the aftermath of the September 11 attacks, the U.S. government dramatically increases funding to stockpile drugs and other agents that could be used to counter a bioterrorism attack.

2002 An explosives-laden boat rams the French oil tanker *Limburg* off the coast of Yemen, killing one member of the tanker's crew, tearing a hole in the vessel and spilling 90,000 barrels of oil. U.S. experts believe that the attack was perpetrated by al-Qaeda members.

2002 Industrialized nations pledge $10 billion to help Russia secure Soviet era nuclear weapons and materials.

2002 The planned destruction of stocks of smallpox-causing Variola virus at the two remaining depositories in the United States and Russia is delayed over fears that large-scale production of vaccine might be needed in the event of a bioterrorist action.

2002 More than 1,300 FBI personnel, along with representatives of other federal, state, and local law enforcement agencies, ensure safety at the 2002 Winter Olympic Games in Salt Lake City. Preparations for the games began in May 1998 and included multiple training exercises involving weapons of mass destruction scenarios.

2002 Scientists at Russia's DS Likhachev Scientific Research Institute for Cultural Heritage and Environmental Protection successfully breed a new kind of highly efficient explosives sniffer dog. The new breed is a cross between a jackal and a Russian Husky.

2002 The Pathogen Genomic Sequencing program is initiated by DARPA to focus on characterizing the genetic components of pathogens in order to develop

diagnostics, treatments and therapies for the diseases they cause.

2002 GAO reports that 13 of the hijackers involved in the September 11 attacks had not been interviewed by U.S. consular officials prior to the granting of visas.

2002 DARPA initiates the Biosensor Technologies program in 2002 to develop fast, sensitive, automatic technologies for the detection and identification of biological warfare agents.

2002 A report released in March by the U.S. National Academy of Sciences Institute of Medicine concludes that AVA anthrax vaccine is "acceptably safe."

2002 Russian and NATO foreign ministers reach final agreement in May on the establishment of the NATO-Russia Council, in which Russia and the 19 NATO countries will have an equal role in decision-making on policy to counter terrorism and other security threats.

2002 NATO secretary-general George Robertson visits Ukrainian capital in July and welcomes Ukraine's declared desire for membership, but he states that further political, economic, and military reforms are necessary before Ukraine can join.

2002 The United States withdraws from the ABM treaty in July.

2002 President Bush calls upon the UN to confront the Iraqi threat and usurp potential Iraqi transfer of weapons of mass destruction to terrorist groups.

2002 On October 1, the U.S. Strategic Command and U.S. Space Command merge to form USSTRATCOM, located at Offutt Air Force Base in Nebraska.

2002 Under threat of serious consequences, including potential military action based on UN Resolution 1441, Iraq allows IAEA's Iraq Action Team to resume inspections in Iraq. The Iraq Action Team is renamed the Iraq Nuclear Verification Office (INVO).

2002 London police arrest seven men in connection with ricin manufacture.

2002 On November 26, President Bush signs into law the Terrorism Risk Insurance Act, intended to cover the private sector in the event of terrorist attacks such as those that occurred on September 11.

2002 Seven countries—Lithuania, Estonia, Latvia, Bulgaria, Romania, Slovakia and Slovenia, are invited to join the European Union at a summit meeting in Prague.

2002 Congress passes and President Bush signs the Homeland Security Act of 2002 into law creating the Department of Homeland Security.

2002 In November, a CIA-operated Predator drone fires a missile that kills Osama bin Laden's top lieutenant in Yemen, Qaed Salim Sinan al-Harethi, and five other al-Qaeda suspects.

2002 A group of Swiss researchers at the Lausanne-based Dalle Molle Institute for Perceptual Artificial Intelligence claim they are 95 percent certain that a tape purported to show Osama Bin Laden and played on Arabic television network Al-Jazeera was a fake. U.S. officials continue to assert that the tape is probably genuine. Investigators claim that the poor tape quality defeats sophisticated efforts using aural spectrogram machines that rely on biometric algorithms to analyze breath patterns, syllable emphasis, frequency of speech, rate of speech, and other factors. Over the next several months, additional tapes are released with experts generally agreeing only that the voice alleged to be that of bin Laden could be genuine. The authenticity of the tapes was critical to determine if the al-Qaeda leader had survived the U.S. war against al-Qaeda in Afghanistan.

2002 Abd al-Rahim al-Nashiri—allegeded to be leader of al-Queda operations in the Persian Gulf—is captured. Nashiri, also known as Abu Asim al-Makki, is suspected of masterminding the October 2000 attack on the USS *Cole.*

2002 Anas al-Liby, one of the FBI's most-wanted fugitives, is captured in Afghanistan. Al-Liby was allegedly linked to the 1998 bombings of American embassies in Kenya and Tanzania.

2002 Ramzi Binalshibh, allegedly one of the most senior al-Qaeda members, is arrested in Pakistan.

2002 Trial of Mounir al-Motassadek begins in Germany. Al-Motassadek, a Moroccan, is the first man to stand trial in the September 11 attacks and is charged with being an accessory to more than 3,000 murders in New York and Washington, and of belonging to an al-Qaeda cell in Hamburg. Motassadek claims he knew the hijackers, but only socially; he is convicted and sentenced to 15 years in prison for being a co-conspirator.

2002 Zacarias Moussaoui, a 34-year-old French citizen of Moroccan origin, is charged with six counts of conspiracy and faces a possible death sentence for alleged involvement in the September 11 attacks. Moussaoui is referred to as the "20th hijacker"; it is suspected that he was unable to participate in the mission because he had been placed under arrest on an unrelated charge. Moussaoui denies involvement in the attacks but admits to being a member of the al-Qaeda network and at his trial publicly supports the actions of the terrorists.

2002 In December, North Korea expels IAEA inspectors, removes surveillance equipment from nuclear facilities, and announces an intent to make plants operational.

2003 Office of Homeland Security becomes Department of Homeland Security on January 24.

2003 President Bush announces formation of Project BioShield during his 2003 State of the Union Address.

2003 Scientists at Sandia National Laboratory report achieving limited controlled fusion using a pulsed power source.

2003 North Korea pulls out of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).

2003 U.S. secretary of state Colin L. Powell presents to the UN Security Council evidence of Iraq's continued development of prohibited biological weapons.

2003 NATO's internal divisions are highlighted as France, Germany, and Belgium temporarily block U.S. moves

to offer military support to Turkey in the event of war in Iraq.

2003 Ten suspected terrorists mysteriously vanish from a high-security prison in Yemen. Among the escapees are two top suspects in the bombing of the USS *Cole.*

2003 Richard Reid, the "shoe bomber" who attempted a suicide bombing of an American Airlines Paris-to-Miami flight in December 2001, pleads guilty on all eight charges against him and declares himself a follower of Osama bin Laden. Reid is sentenced to life in prison without possibility of parole.

2003 U.S. government officials claim that the capture of top al-Qaeda lieutenant Khalid Sheik Mohammed, allegedly al-'s chief operations planner, also yields valuable documents and computer files outlining al-Qaeda operations.

2003 August 19: a truck-bomb explodes near the UN Iraq headquarters in Baghdad, killing 17, including Sergio Vieira de Mello, head of the UN delegation in Iraq.

2003 Virtually all agencies scheduled for transfer to the new Department of Homeland Security are officially moved in a March 1 ceremony attended by President Bush.

2003 Break-up of the space shuttle *Columbia* upon reentry. Scientists use GIS technology to map debris field.

2003 Carbon-graphite coils capable of generating an electromagnetic pulse or otherwise disabling electronics are used in U.S.-led raids on Baghdad, Iraq.

2003 Dolphins and sea lions used in mine detection and swimmer defense in waters off of Iraq.

2003 U.S. intelligence sources indicate that at least 17 nations around the globe have offensive biological weapons programs.

2003 On March 17, U.S. president Bush gives Saddam Hussein and his sons 48 hours to leave Iraq or face war. On March 20, American missiles hit "targets of opportunity" in Baghdad, marking the start of the war to oust Hussein. Intelligence sources on the ground in Iraq have indicated that Hussein and other elements of the Iraqi leadership are meeting in a bunker in Baghdad. In less than 45 minutes, a U.S. B-2 stealth bomber armed with "bunker-buster" munitions attempts to eliminate the Iraqi leadership. For several weeks the fate of Hussein is debated, with Iraqi television showing images of Hussein that do not definitively verify his survival. Within days, U.S. and British ground troops enter Iraq from the south, and on April 9, U.S. forces advance into central Baghdad. Hussein government is toppled, but U.S. efforts to establish order and a new government are hampered by sporadic attacks and sectarian violence.

2003 PLF leader Abu Abbas, found guilty of the murder of an elderly American during the 1985 terrorist hijacking of the cruise ship *Achille Lauro,* is discovered and arrested in Baghdad following Operation Iraqi Freedom.

2003 UN Security Council approves resolution backing the U.S.-led administration in Iraq and plan to lift economic sanctions. U.S. administrator abolishes the Baath Party and security institutions of Saddam Hussein's regime.

2003 August 19: a truck-bomb explodes near the UN Iraq headquarters in Baghdad, killing 17, including Sergio Vieira de Mello, head of the UN delegation in Iraq.

2003 September 23: two U.S. military personnel who have been working at the Guantanamo Bay, Cuba, detention facility, where suspected al-Qaeda members are being held, are accused of espionage.

This page intentionally left blank

Sources

Books

15 Years of Serving the President, 1982–1997. Washington, D.C.: National Security Telecommunications Advisory Committee, 1997.

200th Anniversary of the Office of the Attorney General, 1789–1989. Washington, D.C.: Department of Justice, 1991.

A Cold War Conundrum: The 1983 Soviet War Scare. Washington, D.C.: Center for the Study of Intelligence, 1997.

Abanes, Richard. *American Militias: Rebellion, Racism, and Religion.* Downers Grove, IL: InterVarsity Press, 1996.

Abbott, Patrick. *Airship.* New York: Charles Scribner's Sons, 1973.

Ackerman, S. *Discovering the Brain.* National Academy Press, 1992.

Ackermann, U. *Essentials of Human Physiology.* St. Louis: Mosby Year Book, Inc., 1992.

Adams, Herbert F. R. *SI Metric Units: An Introduction.* Toronto: McGraw-Hill Ryerson, 1974.

Adams, James L. *Flying Buttresses, Entropy, and O-Rings: The World of an Engineer.* Cambridge: Harvard University Press, 1991.

Adams, John A. *Dirt.* College Station, TX: Texas A&M University Press, 1986.

Adams, Raymond D., and Maurice Victor. *Principles of Neurology.* New York: McGraw-Hill, 1989.

Adams-Deschamps, Helene. *Spyglass: An Autobiography.* New York: Holt, 1995.

Aebi, Engel. *Atlas of Microscopy Techniques.* San Diego: Plenum Press, 2002.

Agutter P.S. *Between Nucleus and Cytoplasm.* New York: Chapman and Hall, 1991.

Aharoni, Zvi. Also with: Wilhelm Dietl, Meir Amit, and Helmut Bogler (trans.) *Operation Eichmann: The Truth About the Pursuit, Capture and Trial.* New York: John Wiley and Sons, 1997.

Ahrens, C. David, Rachel Alvelais, and Nina Horne. *Essentials of Meteorology: An Invitation to the Atmosphere.* Belmont, CA: Brooks/Cole, 2000.

Ahrens, C. Donald. *Meteorology Today.* 2d ed. St. Paul, MN: West Publishing Company, 1985.

Ainsworth, Peter B. *Offender Profiling and Crime Analysis.* Portland, OR: Willan, 2001.

Akin, Thomas. *Hardening Cisco Routers.* Sebastopol, CA: O'Reilly, 2002.

Albers, Vernon. *The World of Sound.* Cranbury, NJ: A. S. Barnes and Co., Inc., 1970.

Albert, A.Z. *Quantum Mechanics and Experience.* Cambridge, MA: Harvard University Press, 1992.

Alberts, B., D. Bray, J. Lewis, M. Raff, K. Roberts, and J. Watson, eds. *Molecular Biology of the Cell.* 3d ed. New York: Garland Publishing, 1994.

Alberts, Bruce, Alexander Johnson, Julian Lewis, et al. (eds.) *Molecular Biology of the Cell.* New York: Garland Publishing, 2002.

Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy.* New York: Knopf, 1995.

Aldrich, Richard J. *Intelligence and the War Against Japan: Britain, America, and the Politics of Secret Service.* New York: Cambridge University Press, 2000.

Aldrich, Richard J. *The Hidden Hand: Britain, America, and Cold War Secret Intelligence.* Woodstock, NY: Overlook Press, 2002.

Aleksander, Igor, and Piers Burnett. *Reinventing Man: The Robot Becomes Reality.* New York: Holt, Rinehart and Winston, 1983.

Alexander, John B. *Future War: Non-Lethal Weapons in Twenty-First Century Warfare.* New York: St. Martin's Press, 1999.

Alexander, Martin S. *Knowing Your Friends: Intelligence Inside Alliances and Coalitions from 1914 to the Cold War (Cass Series-Studies in Intelligence).* London; Portland, OR: Frank Cass, 1998.

Alexander, Yonah, and Michael S. Swetnam. *Cyber Terrorism.* Ardsley, NY: Transnational, 2001.

Allen, Edward. *Fundamentals of Building Construction.* 3rd ed. New York, NY: John Wiley & Sons, 1998.

Allen, Edward. *The Architect's Studio Companion.* 3rd ed. New York, NY: John Wiley & Sons, 2001.

Allen, G. D., C. Chui, and B. Perry. *Elements of Calculus.* 2nd ed. Pacific Grove, CA: Brooks/Cole Publishing Co., 1989.

Allen, Garland E., Willliam E. Castle, Charles C. Gillispie, eds. *Dictionary of Scientific Biography,* vol. 3, New York: Scribner, 1971.

Allen, George W. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam.* Chicago: Ivan R. Dee, 2001.

Allen, Oliver E., and the Editors of Time-Life Books. *Planet Earth: Atmosphere.* Alexandria, VA: Time-Life Books, 1983.

Allen, T., and N. Polmar. *Merchants of Treason.* New York: Delacorte Press, 1988.

Alperin, Jonathan. "Groups and Symmetry." In *Mathematics Today,* edited by Lynn Arthur Steen. New York: Springer-Verlag, 1978.

Alvarez, David J. *Allied and Axis Signals Intelligence in World War II.* Portland, OR: F. Cass, 1999.

Alves, Péricles Gasparini. *Prevention of an Arms Race in Outer Space.* New York: United Nations Institute for Disarmament Research, 1991.

Amend, John R., Bradford P. Mundy, and Melvin T. Armold. *General, Organic and Biological Chemistry.* Philadelphia: Saunders, 1990.

American Men and Women of Science: A Biographical Directory of Today's Leaders in Physical, Biological, and Related Sciences, 1998–99, 20th ed. New Providence, NJ: R.R. Bowker, 1998.

American National Standard for Information Sciences: Codes for the Representation of Languages for Information Interchange National Information Standards Organization, 1991.

American Psychiatric Association. *Let's Talk about Psychiatric Drugs.* Washington, DC: American Psychiatric Association, 1993.

American Water Works Association. *Water Quality and Treatment.* 5th ed. Denver: American Water Works Association, 1999.

An Overview of the Emergency Response Program. Washington, D.C.: U.S. Environmental Protection Agency, 1992.

Anastasi, A. *Psychological Testing.* New York: Macmillan, 1982.

Anch, A. Michael et al. *Sleep: A Scientific Perspective.* Englewood Cliffs, NJ: Prentice Hall, 1988.

Anderson, Edwin P. and Rex Miller. *Electric Motors.* New York: Macmillan, 1991.

Anderson, John D. Jr. *Introduction to Flight.* New York: McGraw-Hill, 1989.

Anderson, Malcolm. *Policing the World: Interpol and the Politics of International Police Co-operation.* Oxford: Clarendon Press, 1989.

Anderson, Malcolm. *Policing the World: Interpol and the Politics of International Police Co-operation.* Oxford: Clarendon Press, 1989.

Andreason, N.C., and D.W. Black. *Introductory Textbook of Psychiatry.* Washington, DC: American Psychiatric Press, Inc., 1991.

Andreoli, Thomas E. et al. *Cecil Essentials of Medicine.* Philadelphia: W.B. Saunders Company, 1993.

Andrew, C. *For the President's Eyes Only-Secret Intelligence and the American Presidency from Washington to Bush.* New York: Harper Collins Publishers, 1995.

Andrew, C., and V. Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB.* New York: Basic Books, 1999.

Andrew, Christopher M. *Codebreaking and Signals Intelligence.* Totowa, NJ: F. Cass, 1986.

Andrew, Christopher M. *Her Majesty's Secret Service: The Making of the British Intelligence Community.* New York: Viking, 1986.

Anthony E. Sale, 'The Colossus of Bletchley Park—The German Cipher System', in Raùl Rojas and Ulf Hashagen *The First Computers: History and Architectures*, Cambridge, Massachusetts, MIT Press, 2000.

Arms, Karen, and Pamela S. Camp. *Biology.* 3rd ed. Philadelphia: Saunders College Publishing, 1987.

Armstead, Christopher H., ed. *Geothermal Energy* Paris: UNESCO, 1973.

Aronstein, David C., and Albert C. Piccirillo. *Have Blue and the F-117A: Evolution of the "Stealth Fighter."* Reston, VA: American Institute of Aeronautics and Astronautics, 1997.

ARRL. *The Satellite Experimenter's Handbook.* Radio Society of Great Britain: American Radio Relay League, 1990.

Arson, Ron. *Calculus With Analytic Geometry.* Boston: Houghton Mifflin College, 2002.

Ashbourn, Julian. *Advanced Identity Verification. The Complete Guide.* London: Springer Verlag, 2000.

Asimov, Isaac, and Karen A. Frenkel. *Robots: Machines in Man's Image.* New York: Harmony Books, 1985.

Asimov, Isaac. *Asimov's Biographical Encyclopedia of Science & Technology.* 2nd revised edition. Garden City, NY: Doubleday & Company, Inc., 1982.

Asimov, Isaac. *Asimov's Chronology of Science and Discovery.* New York: Harper & Row, Publishers, 1989.

Asimov, Isaac. *Understanding Physics: Light, Magnetism, and Electricity.* Vol. 2. Signet Science Series. New York: NAL, 1969.

Astor, Gerald. *The "Last" Nazi: The Life and Times of Dr. Joseph Mengele.* New York: Fine, 1985.

Atherly, A.G., J.R. Girton, and J.F. McDonald. *The Science of Genetics.* Fort Worth, TX: Saunders College Publishing, 1999.

Atherton, J.C., and M.J. Blaser, eds. "Helicobacter Infections." *Harrison's Principles of Internal Medicine* New York: McGraw-Hill, 1998.

Atherton, Louise. *SOE Operations in Africa and the Middle East: A Guide to Newly Released Records in the Public Record Office.* London: PRO Publications, 1994.

Atherton, Louise. *SOE Operations in Scandinavia: A Guide to the Newly Released Records in the Public Record Office.* London: PRO Publications, 1994.

Atherton, Louise. *SOE Operations in the Far East: An Introductory Guide to the Newly Released Records of the Special Operations Executive in the Public Record Office.* London: PRO Publications, 1993.

Atherton, Louise. *Top Secret: An Interim Guide to Recent Releases of Intelligence Records at the Public Record Office.* London: PRO Publications, 1993.

Atkins, P. *Quanta: A Handbook of Concepts.* Oxford: Oxford University Press, 1991.

Atkins, P.W. *Molecular Quantum Mechanics,* 2nd ed. Oxford: Oxford University Press, 1983.

Atkins, P.W. *Molecules.* W. H. Freeman, 1987.

Atkins, P.W. *Physical Chemistry,* 6th ed. Oxford: Oxford University Press, 1997.

Atkins, P.W. and J. A. Beran. *General Chemistry,* 2nd edition. New York: Scientific American Books, 1992.

Atkins, Peter W. *The Second Law.* New York: Freeman, 1984.

Atkinson, D.E. *Cellular Energy Metabolism and Its Regulation.* New York: Academic, 1977.

Atkinson, R.L., R.C. Atkinson, E.E. Smith, and D.J. Bem. *Introduction to Psychology.* 10th ed. New York: Harcourt Brace Jovanovich, 1990.

Atlas, R.M. and R. Bartha. *Microbial Ecology.* Menlo Park, CA: Benjamin/Cummings, 1987.

Aubrac, Lucie. Konrad Bieber and Betsy Wing (trans.). *Outwitting the Gestapo.* Lincoln, NB: University of Nebraska Press, 1994.

Ayres, Julia. *Printmaking Techniques.* New York: Watson-Guptill, 1993.

Azaroff, Leonid V. *Elements of X-Ray Crystallography.* New York: McGraw-Hill Book Company, 1968.

Babington-Smith, Constance. *Evidence in Camera: The Story of Photographic Intelligence in World War II.* Newton Abbott, England: David and Charles, 1974.

Babiuk, Lorne A., and John J. Phillips, eds. *Animal Biotechnology.* New York: Pergamon Press, 1989.

Bailey, Brian J. *The Luddite Rebellion.* New York: New York University Press, 1998.

Bailey, James E. *Ullmann's Encyclopedia of Industrial Chemistry.* New York: VCH, 2003.

Bailey, Kathleen C. *Iraq's Asymmetric Threat to the United States and U.S. Allies.* Fairfax, VA: National Institute for Public Policy, 2001.

Bailey, Philip S., Jr., and Christina A. Bailey. *Organic Chemistry: A Brief Summary of Concepts and Applications.* 4th ed. Englewood Cliffs, NJ: Prentice Hall, 1989.

Ball, Desmond. *Politics and Force Levels: The Strategic Missile Program of the Kennedy Administration.* Lexington: University Press of Kentucky, 1988.

Ball, W.W. Rouse. *A Short Account of the History of Mathematics.* London: Sterling Publications, 2002.

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: from the Cold War through the Dawn of a New Century.* New York: Doubleday, 2001.

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency.* Boston: Houghton, Mifflin, 1982.

Bancroft, Mary. *Autobiography of a Spy.* New York: Morrow, 1983.

Banfield, Edwin. *Barometers: Aneroid and Barographs.* Trowbridge, Wiltshire, England: Baros Books, 1985.

Banks, J. Houston. *Elements of Mathematics.* Allyn and Bacon, 1961.

Bar-Joseph, Uri. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain.* University Park: Pennsylvania State University Press, 1995.

Barash, Paul G., Bruce F. Cullen, and Robert K. Stoelting. *Clinical Anesthesia.* Philadelphia, Lippincott, 1992.

Barnes, J. *Basic Geological Mapping,* 3rd ed. New York, John Wiley and Sons, 1995.

Barnett, Raymond & Michael Ziegler. *College Mathematics.* San Francisco: Dellen Publishing Co, 1984.

Baron, Paul A., and Klaus Willeke. *Aerosol Measurement: Principles, Techniques, and Applications.* 2nd ed. Hoboken, NJ: Wiley-Interscience, 2001.

Barrett, E. C., and L. F. Curtis. *Introduction to Environmental Remote Sensing.* New York: Chapman & Hall, 1992.

Barrett, James T. *Textbook of Immunology.* St. Louis: Mosby, 1988.

Barron, James W., Morris H. Eagle, and David L. Wolitzky, eds. *Interface of Psychoanalysis and Psychology.* Washington, D.C.: American Psychological Association, 1992.

Barron, John . *Breaking the Ring.* Boston: Houghton Mifflin, 1987.

Bates, Robert L. *Industrial Minerals: How They Are Found and Used.* Hillside, NJ: Enslow Publishers, Inc., 1988.

Bath, Alan Harris. *Tracking the Axis Enemy: The Triumph of Anglo-American Naval Intelligence.* Lawrence, Kansas: University Press of Kansas, 1998.

Battan, Louis J. *Fundamentals of Meteorology.* Englewood Cliffs, NJ: Prentice-Hall, Inc., 1979.

Beale, Stephen. *Web Tricks and Techniques: Photo Manipulation: Fast Solutions for Hands-On Web Design.* Gloucester: Rockport Publishers, 2002.

Bechthold, W. et al. *Direct Disposal of Spent Nuclear Fuel (Radioactive Waste Management Series).* Graham & Trotman, 1988.

Becker, W., and D. Deamer. *The World of the Cell.* 2nd ed. New York: Benjamin/Cummings, 1990.

Beckett, B. *Introduction to Cryptology.* Malden, Massachusetts: Blackwell Scientific, 1988.

Beckwith, Charlie A., and Donald Knox. *Delta Force.* San Diego: Harcourt Brace Jovanovich, 1983.

Beers, M. H., and R. Berkow, eds. *The Merck Manual of Diagnosis and Therapy.* Whitehouse Station, New Jersey: Merck & Co., Inc., 2002.

Bell, E. T. *Men of Mathematics.* Simon and Schuster, 1961.

Bella J., Edd, and Fapta May Pt. *Amputations and Prosthetics: A Case Study Approach.* 2nd ed. New York: F. A. Davis, 2002.

Bellairs, Angus. *The Life of Reptiles.* Vols. I and II. New York: Universe Books, 1970.

Benenson, A.S. "Giardiasis." *Control of Communicable Diseases Manual.* Washington: American Public Health Association, 1995.

Bennett, J.C., and Cecil F. Plum. *Textbook of Medicine.* Philadelphia: W. B. Saunders Co., 1996.

Bennett, Richard M. *Espionage: An Encyclopedia of Spies and Secrets.* London: Virgin Books, 2002.

Bennis, Warren G., and Patricia Ward Biederman. *Organizing Genius: The Secrets of Creative Collaboration.* Reading, MA: Addison-Wesley, 1997.

Bennish, M.L., and C. Seas. *Current Diagnosis,* vol. 9 Philadelphia: W.B. Saunders Company, 1997.

Benson, Robert Louis. *A History of U.S. Communications Intelligence during World War II: Policy and Administration.* Washington, D.C.: Center for Cryptologic History, National Security Agency, 1997.

Bentley, Tom, and Jon Hastings. *Safe Computing: How to Protect Your Computer, Your Body, Your Data, Your Money and Your Privacy in the Information Age.* Concord, CA: Untechnical Press, 2000.

Berkowitz, Bruce D., and Allan E. Goodman. *Strategic Intelligence for American National Security.* Princeton, NJ: Princeton University Press, 1989.

Berlin, R. E. and C. C. Stanton. *Radioactive Waste Management.* New York: John Wiley & Sons, 1989.

Berne, R. M., and M. N. Levy. *Cardiovascular Physiology.* St. Louis: C. V. Mosby, 1992.

Bernier, Donald R., Paul E. Christian, and James K. Langan, eds. *Nuclear Medicine: Technology and Techniques.* 3rd Edition. St. Louis: Mosby, 1994.

Beschloss, Michael R. *Mayday: Eisenhower, Khruschev and the U-2 Affair.* New York: Harper & Row, 1986.

Best, Richard A. *Project Echelon: U.S. Electronic Surveillance Efforts.* Washington, D.C.: Congressional Research Service, 2000.

Best, Richard A. *The National Security Council: An Organizational Assessment.* Huntington, NY: Novinka Books, 2001.

Best, Richard A., Jr. *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Washington, D.C.: Congressional Research Service, 2001.

Bettelheim, Frederick A., and Jerry March. *Introduction to General, Organic, and Biological Chemistry.* 3rd ed. Fort Worth: Saunders College Publishing, 1991.

Beurton, Peter, Raphael Falk, Hans-Jörg Rheinberger., eds. *The Concept of the Gene in Development and Evolution.* Cambridge, UK: Cambridge University Press, 2000.

Bildstein, Keith L. *White Ibis: Wetland Wanderer.* Washington, D.C.: Smithsonian Institution Press, 1993.

Binns, Tristan Boyer. *The Environmental Protection Agency* Woburn, MA: Heineman Publishers, 2002.

Birdwell, Michael E. *Celluloid Soldiers: The Warner Bros. Campaign Against Nazism.* New York: New York University Press, 1999.

Birkhoff, Garrett, and Saunders MacLane. *A Survey of Modern Algebra.* New York: Macmillan Co., 1947.

Birkhoff, George David, and Ralph Beatley. *Basic Geometry.* New York: Chelsea Publishing Co., 1959.

Birren, Bruce W., and Eric Hon Cheong Lai. *Pulsed Field Electrophoresis: A Practical Guide.* San Diego: Academic Press, 1997.

Bishop, Chris, ed. *The Encyclopedia of Modern Military Weapons: The Comprehensive Guide to over 1,000 Weapon Systems from 1945 to the Present Day.* New York: Barnes & Noble, 1999.

Bishop, Matt.*Computer Security: Art and Science.* Boston: Addison Wesley Professional, 2002.

Bittar, F. Edward, ed. *Chemistry of the Living Cell.* Greenwich, CT: JAI Press, 1992.

Bittinger, Marvin L, and Davic Ellenbogen. *Intermediate Algebra: Concepts and Applications.* 6th ed. Reading, MA: Addison-Wesley Publishing, 2001.

Bixler, Margaret T. *Winds of Freedom: The Story of the Navajo Code Talkers of World War II.* Darien, CT: Two Bytes Publishing Company, 1992.

Black, Ian and Benny Morris. *Israel's Secret Wars: A History of Israel's Intelligence Services.* New York: Grove Press, 1992.

Blackstock, Paul W., and Frank L. Schaf, Jr., eds. *Intelligence, Espionage, Counterespionage, and Covert Operations: A Guide to Information Sources.* Detroit, MI: Gale Research Company, 1978.

Blair, Clay. *The Forgotten War: America in Korea, 1950–1953.* New York: Times Books, 1987.

Blake, Bernard, ed. *Jane's Radar and Electronic Warfare Systems.* Alexandria, VA: Jane's Information Group Inc., 1992.

Bland W., and D. Rolls. *Weathering, an Introduction to Scientific Principles.* New York: Oxford University Press, 1988.

Blight J.G., and D.A. Welch. *Intelligence and the Cuban Missile Crisis.* London; Portland, OR: Frank Cass, 1998.

Blight, James, and Peter Kornbluh. *Politics of Illusion: The Bay of Pigs Invasion Reexamined.* Boulder, CO: Lynne Rienner Publishers, 1998.

Bloomfield, Louis A. *How Things Work: The Physics of Everyday Life.* 2nd ed. New York: John Wiley & Sons, 2000.

Bloss, F. D. *Crystallography and Crystal Chemistry.* New York: Holt, Rinehart and Winston, Inc., 1971.

Blum, Howard. *I Pledge Allegiance.* New York: Simon and Schuster, 1987.

Blunden, Bob. *The Money Launderers: How They Do It, and How to Catch Them at It.* Chalford, England: Management Books, 2001.

Blyth, Andrew and Gerald L. Kovacich. *Information Assurance: Surviving in the Information Environment.* London: Springer, 2001.

Bock, G., G. Cardew, and H. Paretzhe, eds. *Health Impacts of Large Releases of Radionucludes.* John Wiley and Sons, 1997.

Bockris, John O'M., and Amulya K. N. Reddy. *Modern Electrochemistry.* New York: Plenum Press, 1973.

Bodziak J., and Jon J. Nordby *Forensic Science: An Introduction to Scientific and Investigative Techniques.* CRC Press, 2002.

Boehm, Roy, and Charles W. Sasser. *First SEAL.* New York: Pocket Books, 1997.

Boggs., Sam, Jr. *Principles of Sedimentology and Stratigraphy,* 2nd edition. Englewood Cliffs, NJ: Prentice Hall, 1995.

Bohr, Niels. *The Unity of Knowledge.* New York: Doubleday & Co., 1955.

Bohrer, David. *America's Special Forces.* St. Paul, MN: MBI Publishing, 2002.

Boikess, Robert S., and Edward Edelson. *Chemical Principles.* 2nd edition. New York: Harper & Row Publishers, 1981.

Bolemon, Jay. *Physics: A Window On Our World,* 3rd ed. Needham, MA: Prentice-Hall, 1995.

Bolin, Robert L. *Technical Intelligence Bibliography.* Athens, GA: University of Georgia, Political Science Department, 1985.

Boll, Michael M. *National Security Planning Roosevelt through Reagan.* Lexington: University Press of Kentucky, 1988.

Bolz, Frank, et al. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques.* Boca Raton, FL: CRC Press, 2002.

Bonds, Ray, ed. *The Modern U.S. War Machine: An Encyclopedia of American Military Equipment and Strategy.* New York: Military Press, 1987.

Boorse, Henry A., Lloyd Motz, and Jefferson Hane Weaver. *The Atomic Scientists: A Biographical History.* New York: John Wiley & Sons, Inc., 1989.

Bord, Donald J. and Vern J. Ostdiek. *Inquiry Into Physics.* 3rd ed. West Publishing Company, 1995.

Born, Max, and Emil Wolf. *Principles of Optics.* New York: Pergamon Press, 1980.

Borosage, Robert, and John D. Marks. *The CIA File.* New York: Grossman, 1976.

Borth, Christy. *Mankind on the Move: The Story of Highways.* Automotive Safety Federation, 1969.

Bosiljevac, T. J. *SEALs: UDT/SEAL Operations in Vietnam.* New York: Ivy Books, 1991.

Boss, Martha J., Dennis W. Day, and Roger F. Jones. *Biological Risk Engineering Handbook: Infection Control and Decontamination.* Boca Raton: Lewis Publishers, Inc., 2002.

Bossler, John D., John R. Jensen, Chris McMaster, and Chris Rizos, (eds). *Manual of Geospatial Science and Technology.* Mount Laurel, New Jersey: Taylor & Francis, 2001.

Bosworth, Seymour (ed.), and Michel E. Kabay. *Computer Security Handbook.* New York: John Wiley & Sons, 2002.

Bourret, Jean Claude. *GIGN, Vingt Ans D'Actions: 1974–1994.* Paris: M. Lafon, 1995.

Bouvier, Virginia Marie. *Whose America? The War of 1898 and the Battles to Define the Nation.* Westport, CT: Praeger, 2001.

Bowditch, W., and K. Bowditch. *Welding Technology Fundamentals.* South Holland, IL: Goodheart-Willcox, 1992.

Boyd, Richard H., and Paul J. Phillips. *The Science of Polymer Molecules.* Cambridge University Press, 1996.

Boyd, T. J. M., and J. J. Anderson. *The Physics of Plasma.* Cambridge, UK: Cambridge University Press, 2003.

Boyer, Carl B. *A History of Mathematics.* 2nd ed. Revised by Uta C. Merzbach. New York: John Wiley and Sons, 1991.

Boyle, Robert. *Gold History and Genesis of Deposits.* New York: Van Nostrand Reinhold, 1987.

Boylstad, Robert, and Louis Nashalsky. *Electronics: A Survey.* Englewood Cliffs, NJ: Prentice Hall, 1985.

Boyne, Walter J. *Beyond the Wild Blue: A History of the United States Air Force, 1947–1997.* New York: St. Martin's Press, 1997.

Boyne, Walter J. *Boeing B-52: A Documentary History.* New York: Jane's, 1982.

Brady, G. S., and H. R. Clause. *Materials Handbook.* New York: McGraw Hill, Inc, 1991.

Brady, James E. and John R. Holum. *Fundamentals of Chemistry.* New York: Wiley, 1988.

Brady, Russell, and John R. Holum. *Chemistry, Matter and Its Changes.* 3rd ed. New York: John Wiley and Sons Inc., 2000.

Bramwell, Martyn. *Weather.* New York: Franklin Watts, 1994.

Branden, C., and J. Tooze. *Introduction to Protein Structure.* New York: Garland, 1991.

Brandrup, J., and E. H. Immergut, eds. *Polymer Handbook.* 3rd Edition. New York, NY: Wiley-Interscience, 1990.

Branscomb, Anne W. *Who Owns Information? From Privacy to Public Access.* New York: Basic Books, 1994.

Breckenridge, Robert P. *Modern Camouflage, the New Science of Protective Concealment.* New York: Farrar & Rinehart, 1942.

Breckinridge, Scott D. *The CIA and the U.S. Intelligence System.* Boulder, CO: Westview Press, 1986.

Bresler, Fenton. *Interpol.* London: Sinclair-Stevenson, 1992.

Briggs, S.A. *Basic Guide to Pesticides. Their Characteristics and Hazards.* Washington, D.C.: Taylor & Francis, 1992.

Brill, A. B., et al. *Low-level Radiation Effects: A Fact Book.* New York: The Society of Nuclear Medicine, 1985.

Brock, William H. *The Norton History of Chemistry.* New York: W. W. Norton & Company, 1993.

Brockris, J. O'M. *Energy Options.* Redfern NSW, Australia: Halsted Press, 1980.

Brodie, Bernard and Fawn M. Brodie. *From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare.* Bloomington, IN: Indiana University Press, 1973.

Brombacher, W. G. *Mercury Barometers and Manometers.* Washington, D.C.: U.S. Department of Commerce, National Bureau of Standards, 1960.

Brooker, R. *Genetics Analysis and Principals.* Menlo Park: Benjamin Cummings, 1999.

Brooks, J. *Telephone: The First Hundred Years.* Harper & Row, 1976.

Browder, George C. *Hitler's Enforcers: The Gestapo and SS Security Service in the Nazi Revolution.* Oxford: Oxford University Press, 1996

Brown, Anthony Cave. *The Last Hero: Wild Bill Donovan.* New York: Times Books, 1982.

Brown, Harold, and Franklin Neva. *Basic Clinical Parasitology.* Norwalk, CT: Appleton-Century-Crofts, 1983.

Brown, Julian. *Minds, Machines, and the Multiverse: The Quest for the Quantum Computer.* New York: Simon & Schuster, 2000.

Brown, William H., and Elizabeth Rogers. *General, Organic and Biochemistry.* Boston: Willard Grant, 1980.

Browne, J. P. R. *Electronic Warfare.* London: Brassey's, 1998.

Brugioni, Dino A. *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis.* New York: Random House, 1990.

Brugioni, Dino A. *From Balloons to Blackbirds: Reconnaissance, Surveillance and Imagery Intelligence: How It Evolved.* McLean, VA: Association of Former Intelligence Officers, 1993.

Brugioni, Dino A. *Photo Fakery: The History and Techniques of Photographic Deception.* Washington, D.C.: Brassey's, 1999.

Bruice, Paula. *Organic Chemistry.* 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 2001.

Buchanan, B. B., W. Gruissem, and R. L. Jones. *Biochemistry and Molecular Biology of Plants.* Rockville, MD: American Society of Plant Physiologists, 2000.

Buchanan, R.E., and N.E. Gibbons. *Bergey's Manual of Determinative Bacteriology,* 8th ed. Baltimore: The Williams & Wilkins Company, 1974.

Buck, Alice L. *A History of the Atomic Energy Commission.* U.S. Department of Energy, 1983.

Budavari, Susan, editor. *The Merck Index.* Merck Research Laboratories, 1996.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II.* New York: Touchstone Books, 2002.

Buechel, K.H., et al. *Industrial Inorganic Chemistry.* New York: VCH, 2000.

Buelow, George, and Suzanne Hebert. *Counselor's Resource on Psychiatric Medications, Issues of Treatment and Referral.* Pacific Grove, CA: Brooks/Cole, 1995.

Buranelli, Vincent, and Nan Buranelli. *Spy Counterspy: An Encyclopedia of Espionage.* New York: McGraw-Hill, 1982.

Bureau of Alcohol, Tobacco, and Firearms: Its History, Progress, and Programs. Washington, D.C.: U.S. Government 1995.

Burn R. P. *A Pathway Into Number Theory.* 2nd. ed. New York: Cambridge University Press, 1997.

Burnham, David. *A Law unto Itself: Power, Politics, and the IRS.* New York: Random House, 1989.

Burrough, P.A. and R.A. McDonnell. *Principles of Geographic Information Systems,* 2nd ed. Oxford: University Press, 1998.

Burrows, William E. *By Any Means Necessary: America's Secret Air War in the Cold War.* New York: Farrar, Straus and Giroux, 2001.

Burrows, William. *Deep Black: Space Espionage and National Security.* New York: Random House, 1986.

Burton, David M. *The History of Mathematics,* 5th Ed. New York: McGraw Hill College Division, 2002.

Busby, Robert. *Reagan and the Iran-Contra Affair.* Chippenham, Wiltshire, Great Britain: Macmillan, 1999.

Bushart, Howard L. *Soldiers of God: White Supremacists and Their Holy War for America.* New York: Kensington, 1998.

Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security.* New York: Public Affairs, 2001.

Bynum, W. F., E. J. Browne, and Roy Porter. *Dictionary of the History of Science.* Princeton, NJ: Princeton University Press, 1981.

Cabinet Office. *National Intelligence Machinery.* London: HMSO, 2000.

Cahill, M. *Handbook of Diagnostic Tests.* Springhouse Company, 1995.

Cairns, J., G. S. Stent, and J. D. Watson, eds. *Phage and the Origins of Molecular Biology,* 2nd ed. New York: Cold Spring Harbor Laboratory of Quantitative Biology, 1992.

Calder, James, comp. *Intelligence, Espionage and Related Topics: An Annotated Bibliography of Serial Journal and Magazine Scholarship, 1844–1998.* Westport, CT: Greenwood, 1999.

Calhoun, Frederick S. *The Trainers: The Federal Law Enforcement Training Center and the Professionalization of Federal Law Enforcement.* Washington, D.C.: U.S. Government Printing Office, 1996.

Cameron, Gavin. *Nuclear Terrorism: A Threat Assessment for the 21st Century.* New York: St. Martin's Press, 1999.

Campbell, A. M. "Monoclonal Antibodies." In *Immunochemistry,* edited by Carol J. van Oss and Marc H. V. van Regenmortel. New York: Marcel Dekker, Inc., 1994.

Campbell G.L., and D.T. Dennis. "Plague and other Yersinia Infections." In: Kasper DL, et al; eds. *Harrison's Principles of Internal Medicine,* 14th ed. New York: McGraw Hill, 1998.

Campbell, James B. *Introduction to Remote Sensing (3rd edition).* New York: Guilford Press, 2002.

Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign Against Terrorism.* Washington, D.C.: CSIS Press, 2001.

Campbell, N., J. Reece, and L. Mitchell. *Biology.* 5th ed. Menlo Park: Benjamin Cummings, Inc., 2000.

Cannon, Don L. *Understanding Solid-State Electronics.* 5th ed. SAMS division of Prentice Hall Pub. Co., 1991.

Canton, Bruce. *The Civil War.* American Heritage/Wings Books, New York/Avenel, NJ, 1960.

Cantor, Norman F. *In the Wake of the Plague: The Black Death and the World It Made.* New York: Perennial, 2002.

Cantwell, John D. *The Second World War: A Guide to Documents in the Public Record Office.* London: PRO, 1998.

Caplan, Arthur L., ed. *When Medicine Went Mad: Bioethics and the Holocaust.* Totowa, N.J.: Humana, 1992.

Carey, Francis A., and Richard J. Sundberg. *Advanced Organic Chemistry: Structure and Mechanisms.* 4th ed. New York: Plenum, 2001.

Carey, Joseph, ed. *Brain Facts, A Primer on the Brain and the Nervous System.* Washington, D.C.: Society for Neuroscience, 1993.

Carl, Leo D. *The CIA Insider's Dictionary of U.S. and Foreign Intelligence, Counterintelligence, and Tradecraft.* Washington, D.C.: NIBC Press, 1996.

Carlisle, Rodney P. *Encyclopedia of the Atomic Age.* New York: Facts on File, 2001.

Carlisle, Rodney P., with Joan M. Zenzen. *Supplying the Nuclear Arsenal: American Production Reactors, 1942–1992.* Baltimore: John Hopkins University Press, 1996.

Carney, John T., and Benjamin F. Schemmer. *No Room for Error: The Covert Operations of America's Special Tactics Units from Iran to Afghanistan.* New York: Ballantine, 2002.

Caro, Paul. *Water.* New York: McGraw Hill, 1993.

Carroll, Felix A. *Perspectives on Structure and Mechanism in Organic Chemistry.* Pacific Grove, CA: Brooks/Cole Publishing Company, 1998.

Carroll, Peter N. *It Seemed Like Nothing Happened: America in the 1970s.* New Brunswick: Rutgers University Press, 1990.

Carter, Richard. *Breakthrough: The Saga of Jonas Salk.* Naples, FL: Trident Press, 1966.

Cassaro, Edward, and Linda Lomonaco. *Operators Guide: Atmospheric Release Advisory Capability (ARAC) Site Facility.* Springfield, VA: Department of Energy, 1979.

Causewell, Erin V. *National Missile Defense: Issues and Developments.* New York: Novinka Books, 2002.

Cefrey, Holly, et al. *Epidemics: Deadly Diseases Throughout History (The Plague, AIDS, Tuberculosis, Cholera, Small Pox, Polio, Influenza, and Malaria.* New York: Rosen Publishing Group, 2001.

Chalker, Dennis C., and Kevin Dockery. *One Perfect Op: An Insider's Account of the Navy SEAL Special Warfare Teams.* New York: Morrow, 2002.

Chalou, George C. *Scientific and Technical Intelligence Gathering.* New York: Garland Publishing, 1989.

Chalou, George C. *The Secrets of War: The Office of Strategic Services in World War II.* Washington, D.C.: National Archives and Records Administration, 1992.

Chandrasekhar, S. *Liquid Crystals.* 2nd. ed. Cambridge University Press, 1992.

Chang, Laurence, ed.*Cuban Missile Crisis, 1962: A National Security Archive Documents Reader (National Security Archive Documents Reader)* Wasingtion, D.C.: United States Government Press, 1998.

Chang, Raymond. *Chemistry.* New York: McGraw-Hill, 1991.

Chant, Christopher. *The Encyclopedia of Codenames of World War II.* London: Routledge & Kegan Paul, 1986.

Chant, Christopher. *An Illustrated Data Guide to Modern Reconnaissance Aircraft.* London: Tiger Books International, 1997.

Chapman, Robert, et. al. *COPS Innovations: A Closer Look: Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness.* Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services.

Charthouse, Robert. *Codes and Ciphers.* Cambridge, England: Cambridge University Press, 2002.

Chen, C. H. *Information Processing for Remote Sensing.* River Edge, NJ: World Scientific, 1999.

Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin.*Firewalls and Internet Security: Repelling the Wiley Attacker,* 2nd edition. Boston: Addison Wesley Professional, 2003.

Cheung, Kin P. *Plasma Charging Damage.* Berlin: Springer Verlag, 2000.

Chikazumi, S. *Physics of Magnetism.* New York: John Wiley & Sons, Ltd., 1984.

Child, Graham. *Sound.* Garden City, NY: Doubleday Science Series, Doubleday and Company, Inc., 1970.

Chin, J. "Tularemia." In *Control of Communicable Diseases Manual.* Washington, D.C.: American Public Health Association, 2000.

Chrzanowski, Edward J. *Active Radar Electronic Countermeasures.* Norwood, MA: Artech House, 1990.

CIA History Staff. *CIA Cold War Records: CORONA—America's First Satellite Program.* Washington, D.C., 1995.

CIA History Staff. *CIA Cold War Records: The CIA Under Harry Truman.* Washington, D.C.: CIA, 1994.

Cimbala, Stephen J. *Nuclear Strategy in the Twenty-First Century.* Westport, CT: Praeger, 2000.

Cirincione, Joseph, Jon B. Wolfsthal, Miriam Rajkuman, and Jessica T. Mathews. *Deadly Arsenals: Tracking Weapons of Mass Destruction.* Washington, D.C.: Carnegie Endowment for International Peace, 2002.

Clancy, Tom. *Carrier: A Guided Tour of an Aircraft Carrier.* New York: Berkley Books, 1999.

Clancy, Tom. *Fighter Wing: A Guided Tour of an Air Force Combat Wing.* New York: Berkley Books, 1995.

Clark, Wesley K. *Waging Modern War: Bosnia, Kosovo, and the Future of Combat.* New York: Public Affairs, 2001.

Clarke, C. A. *Human Genetics and Medicine,* 3rd ed. Baltimore, MD: E. Arnold, 1987.

Cleroux, Richard. *Official Secrets: The Story Behind the Canadian Security Intelligence Service.* Toronto: McGraw-Hill Ryerson, 1990.

Closing the Circle on the Splitting of the Atom: The Environmental Legacy of Nuclear Weapons Production in the United States and What the Department of Energy Is Doing About It. Washington, D.C.: U.S. Government Printing Office, 1995.

Clydesdale, Fergus, ed. *Food Science and Nutrition: Current Issues and Answers.* Englewood Cliffs, N.J.: Prentice-Hall, 1979.

Cobb, Cathy, and Harold Goldwhite. *Creations of Fire: Chemistry's Lively History from Alchemy to the Atomic Age.* New York: Plenum Press, 1995.

Cochran, Thomas B., William M. Arkin, and Milton M. Hoenig. *Nuclear Weapons Databook: Vol. I, U.S. Nuclear Forces and Capabilities.* Cambridge, MA: Ballinger Publishing Company, 1984.

Coggins, Jack. *Arms and Equipment of the Civil War.* Wilmington, NC: Broadfoot Publishing Company, 1990.

Cohen, Susan, and Daniel Cohen. *Pan Am 103: The Bombing, the Betrayals, and the Bereaved Families' Search for Justice.* New York: Signet, 2001.

Cohn, Victor. *News and Numbers. A Guide to Reporting Statistical Claims and Controversies in Health and Related Fields.* Ames: Iowa State University Press, 1989.

Colby, William E. *Honorable Men—My Life in the CIA.* New York: Simon and Schuster, 1978.

Colby, William E., with James McCarger. *Lost Victory: A Firsthand Account of America's Sixteen-Year Involvement in Vietnam.* Chicago: Contemporary Books, 1989.

Cole, Leonard A. *The Eleventh Plague: The Politics of Biological and Chemical Warfare.* New York: WH Freeman and Company, 1996.

Colliers, A,. et al. *Microbiology and Microbiological Infections,* vol. 3. London: Edward Arnold Press, 1998.

Collin, Richard H. *Theodore Roosevelt's Caribbean: The Panama Canal, the Monroe Doctrine, and the Latin American Context.* Baton Rouge: Louisiana State University Press, 1990.

Collings, Peter J. *Liquid Crystals: Nature's Delicate Phase of Matter.* Princeton University Press, 1990.

Collins, A. Frederick. "Vacuum Tubes." *The Radio Amateur's Handbook.* revised by Robert Herzberg. New York: Harper & Row, 1983.

Collins, A. G., and A. I. Johnson, eds. *Ground-Water Contamination: Field Methods.* Philadelphia: American Society for Testing and Materials, 1988.

Collins, Mark, ed. *The Last Rain Forests.* London: Mitchell Beazley Publishers, 1990.

Combatting Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism. Washington, D.C.: General Accounting Office, 2000.

Comer, Ronald J. *Abnormal Psychology.* 2nd ed. New York: W. H. Freeman, 2000.

Communications Management and Control Activity (CMCA). Washington, D.C.: Defense Information Systems Agency, 1995.

Conboy, Kenneth J. *Feet to the Fire: CIA Covert Operations in Indonesia.* Annapolis MD: Naval Institute Press, 1999.

Conboy, Kenneth J., and Dale Andradé. *Spies and Commandos: How America Lost the Secret War in North Vietnam.* Lawrence, KS: University Press of Kansas, 2000.

Conboy Kenneth J., and J. Morrison. *The CIA's Secret War in Tibet.* Lawrence, KS: University Press of Kansas, 2002.

Congressional Research Service. *The United States Intelligence Community: A Brief Description of Organization and Functions.* Washington, D.C.: Library of Congress, 1975.

Connors, Edward F. *Convicted by Juries, Exonerated by Science: Case Studies in the Use of DNA Evidence to Establish Innocence After Trial.* Washington, D.C.: National Institute of Justice, 1996.

Conroy, John. *Unspeakable Acts: The Dynamics of Torture.* New York: Alfred A. Knopf, 2000.

Constantinides, George C. *Intelligence and Espionage: An Analytical Bibliography.* Boulder, CO.: Westview Press, 1983.

Cook, Don. *Forging the Alliance: The Birth of the NATO Treaty and the Dramatic Transformation of U.S. Foreign Policy Between 1945 and 1950.* New York: Arbor House/William Morrow, 1989.

Cord Meyer. *Facing Reality: From World Federalism to the CIA.* New York: Harper & Row, 1980.

Cordesman, Anthony H. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

Cormican, M. G. and M. A. Pfaller. "Molecular Pathology of Infectious Diseases." *Clinical Diagnosis and Management by Laboratory Methods.* 20th ed. Philadelphia: W. B. Saunders, 2001.

Corvo, Max. *The O.S.S. in Italy, 1942–1945: A Personal Memoir.* New York: Praeger, 1990.

Cotran, Ramzi S., et al. *Robbins Pathologic Basis of Disease.* Philadelphia: W. B. Saunders Company, 1994.

Coughlan, G. D. and J. E. Dodd. *The Ideas of Particle Physics.* 2nd ed. Cambridge: Cambridge University Press, 1991.

Courant, Richard, and Herbert Robbins. *What Is Mathematics?* Oxford: Oxford University Press, 1948.

Couzens, E. G. and V. E. Yarsley. *Plastics in the Modern World.* Baltimore, MD: Penguin, 1968.

Cowan, Henry J. *The Master Builders.* New York: Wiley, 1977.

Crabb, Cecil V. and Kevin V. Mulcahy. *American National Security: A Presidential Perspective.* Pacific Grove, CA: Brooks/Cole, 1991.

Craft, B.C. *Applied Petroleum Reservoir Engineering,* 2nd Edition. Englewood Cliffs, NJ: Prentice Hall, Inc., 1991.

Craig, Gordon Alexander, and Francis J. Lowenheim. *The Diplomats, 1939–1979.* Princeton, NJ: Princeton University Press, 1994.

Craig, James, David Vaughan, and Brian Skinner. *Resources of the Earth.* Englewood Cliffs, New Jersey: Prentice Hall, 1988.

CRC Handbook of Chemistry and Physics. Boston: CRC Press, Inc., published yearly.

Crickmore, Paul F. *Lockheed SR-71: The Secret Missions Exposed.* London: Osprey, 1988.

Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C.: The Commission, 1997.

Croall, C., and S. Sempler. *Nuclear Power for Beginners.* New York: State Mutual Books, 1990.

Cross, Wilbur. *Petroleum.* Chicago: Children's Press, 1983.

Cumpsty, Nicholas A. *Jet Propulsion : A Simple Guide to the Aerodynamic and Thermodynamic Design and Performance of Jet Engines.* Cambridge: Cambridge University Press, 1998.

Curtis, A. R. *Space Almanac.* Arcsoft Publishers, 1990.

Cutnell, John D., and Kenneth W. Johnson. *Physics.* 3rd ed. New York: Wiley, 1995.

Dahl, Per F. *Heavy Water and the Wartime Race for Nuclear Energy.* Bath, UK: Institute of Physics Publishing, 1999.

Daintith, John and D. Gjertsen, eds. *A Dictionary of Scientists.* New York: Oxford University Press, 1999.

Dallas, Gregor. *The Final Act: the Roads to Waterloo.* New York: Henry Holt and Co., 2001.

Dalton, Patricia A. *Combating Terrorism: Enhancing Partnerships through a National Preparedness Strategy.* Washington, D.C.: General Accounting Office, 2002.

Danaher, Kevin, editor. *Fifty Years is Enough: The Case Against the World Bank and the International Monetary Fund.* Cambridge, MA: South End Press, 1994.

Danby, J. M. A. *Computer Modeling: From Sports to Spaceflight—From Order to Chaos.* Richmond, VA: Willmann-Bell, 1997.

Dando, Malcolm. *Biological Warfare in the 21st Century.* New York: Macmillan, 1994.

Danielson, Eric W., James Levin, and Elliot Abrams. *Meteorology.* 2nd ed. with CD-ROM. Columbus: McGraw-Hill Science/Engineering/Math, 2002.

Dantzig, Tobias. *Number, the Language of Science.* Garden City, NY: Doubleday and Co., 1954.

Darby, N. J., and T. E. Creighton. *Protein Structure.* New York: Oxford University Press, 1994.

Darling, Arthur. *The Central Intelligence Agency An Instrument of Government to 1950.* State College: Pennsylvania State University Press, 1990.

Darnell, J., H. Lodish, and D. Baltimore. *Molecular Cell Biology.* New York: Scientific American Books, Inc., 1986.

Das, Ashok and Thomas Ferbel. *Introduction to Nuclear and Particle Physics.* John Wiley, 1994.

Daughtery, William J. *In the Shadow of the Ayatollah: A CIA Hostage in Iran.* Annapolis, MD: Naval Institute Press, 2001.

Davenport, Harold. *The Higher Arithmetic: An Introduction to the Theory of Numbers.* 6th edition. Cambridge: Cambridge University Press, 1992.

Davidovits, Peter. *Communication.* New York: Holt, Rinehart and Winston, Inc., 1972.

Davies, Philip H. J. *The British Secret Services.* Brunswick, NJ: Transaction Publishers, Rutgers University, 1996.

Davis, Brian L. *Qaddafi, Terrorism, and the Origins of the U.S. Attack on Libya.* New York: Praeger, 1990.

Davis, Charles O. *Across the Mekong: The True Story of an Air America Helicopter Pilot.* Hildesigns Press, 2000.

Davis, James Kirkpatrick. *Spying on America: The FBI's Domestic Counterintelligence Program.* New York: Praeger, 1992.

Davis, Joel. *Mapping the Code: The Human Genome Project and the Choices of Modern Science.* Wiley, 1990.

Davis, Richard A., Jr. *Oceanography, An Introduction to the Marine Environment.* Dubuque, IA: William C. Brown Publishers, 1991.

Davis, S. N., and R. J. M. DeWiest. *Hydrogeology.* New York: Wiley, 1966.

Davis, Shelley L. *Unbridled Power: Inside the Secret Culture of the IRS.* New York: HarperBusiness, 1997.

Day, Dwayne A., and John M. Logsdon. *Eye in the Sky: The Story of the Corona Spy Satellites.* Washington, D.C.: Smithsonian Institution Press, 1998.

De Bono, Edward. *Eureka! An Illustrated History of Inventions From the Wheel to the Computer.* London: Thames and Hudson, 1974.

De Gennes, P.G., and J. Prost. *The Physics of Liquid Crystals.* 2nd. ed. Oxford Science Publications, 1993.

De Riaz, Yvan A. *The Book of Knives.* New York: Crown, 1981.

Dean, John A., ed. *Lange's Handbook of Chemistry.* 15th ed. New York: McGraw-Hill, 199.

Deavours, Cipher, et al. *Cryptology: Machines, History & Methods.* Norwood, MA: Artech House, 1989.

The Defense Information Systems Agency (DISA): NAA, "The Three Sisters." Washington, D.C.: Defense Information Systems Agency, 1995.

Dehqanzada, Yahya A., and Ann Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World.* Washington, D.C.: Carnegie Endowment for International Peace, 2000.

Del Bimbo, Alberto. *Visual Information Retrieval.* San Fransisco: Morgan Kaufmann Publishers, 1999.

Delaney, C. F. G., and E. C. Finch. *Radiation Detectors.* New York: Oxford University Press, 1992.

Delaporte, François. *Disease and Civilization: The Cholera in Paris, 1832.* Cambridge: MIT Press, 1986.

The Department of Justice Manual. Gaithersburg, MD: Aspen Law & Business, 2000.

Department of the Treasury. *Excerpts from the History of the United States Secret Service, 1865–1875.* Washington, D.C.: Department of the Treasury, 1978.

Deriabin J.L., and P. Deriabin. *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War.* New York: Scribner's, 1992.

Dessler, A. *The Chemistry and Physics of Stratospheric Ozone.* Cornwall, UK: Academic Press, 2000.

Devore, Ronald M. *Spies and All That: Intelligence Agencies and Operations; A Bibliography.* Los Angeles: California State University, Center for the Study of Armament and Disarmament, 1977.

DeVorkin, D. H. *Race to the Stratosphere.* Springer-Verlag, 1989.

Diagnostic and Statistical Manual of Mental Disorders, DSM-IV. Washington, DC: American Psychiatric Association, 1994.

Dickson, Leonard Eugene. *History of the Theory of Numbers.* Providence, RI: American Mathematical Society, 1999.

Dickson, T.R. *Introduction to Chemistry.* Wiley and Sons, 1991.

Diffie, Whitfield, and Susan Eva Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, MA: MIT Press, 1998.

D'Ignazio, Fred. *Working Robots.* New York: Elsevier/Nelson Books, 1982.

Disclosure of Classified Information to Congress. Washington, D.C.: U.S. Government Printing Office, 1998.

Disposition of Production Records of the Defense Intelligence Agency: A NARA Evaluation. Washington, D.C.: National Archives and Records Administration, 1996.

Dixon, Dougal, and Raymond L. Bernor, ed. *The Practical Geologist.* New York: Simon and Schuster, 1992.

Dobson, C., R. Payne. *War Without End: The Terrorists, An Intelligence Dossier.* London: Harrap Limited, 1986.

DOD Investigation Programs: Background Data. Washington, D.C.: United States General Accounting Office 1989.

Doerfler, Walter, and Petra Bohm, eds. *Virus Strategies: Molecular Biology and Pathenogenesis.* New York: VCH, 1993.

Doremus, R. H. *Glass Science.* New York: Wiley, 1990.

Dorril, Stephen. *MI6: Inside the Cover World of Her Majesty's Secret Intelligence Service.* New York: Free Press, 2000.

Dorwart, Jeffery M. *The Office of Naval Intelligence: The Birth of America's First Intelligence Agency, 1865–1918.* Annapolis, MD: Naval Institute Press, 1979.

Doyle, M.P., and V.S. Padhye. *Escharichia coli In Foodborne Bacterial Pathogens.* New York: Marcel Dekker, Inc., 1989.

Drell, S.D. *The New Terror: Facing the Threat of Biological and Chemical Weapons.* Stanford, CA: Hoover Institute Press, 1999.

Drell, Sidney D., Philip J. Farley, and David Holloway. *The Reagan Strategic Defense Initiative: A Technical, Political, and Arms Control Assessment.* Cambridge, MA: Ballinger Publishing Co, 1990.

Drew, W. Lawrence. "Chlamydia." *Sherris Medical Microbiology: An Introduction to Infectious Diseases,* 3rd ed. Ed. Kenneth J. Ryan. Norwalk, CT: Appleton & Lange, 1994.

Duffner, Robert. *Airborne Laser: Bullets of Light.* New York: Plenum Trade, 1997.

Dulles, Allen. *The Craft of Intelligence.* New York: Harper and Row, 1963.

Dunlop, John. *Automation and Technological Change.* Englewood Cliffs, NJ: Prentice-Hall, 1962.

Durant, Will and Ariel. *The Age of Napoleon.* New York: Simon and Schuster, 1975.

Dwyer, Jim. *Two Seconds under the World: Terror Comes to America.* New York: Crown Publishers, 1994.

Dyson, Norman A. *X Rays in Atomic and Nuclear Physics.* White Plains, NY: Longman, 1973.

Dziak, John J. *Chekisty: A History of the KGB.* Massachusetts: D. C. Heath and Company, 1988.

Eagleman, Joe R. *Meteorology: The Atmosphere in Action.* 2nd ed. Belmont, CA: Wadsworth Publishing Company, 1985.

Earley, Pete. *Confessions of a Spy: The Real Story of Aldrich Ames.* New York: G.P. Putnam's Sons, 1997.

Ebbing, Darrell. *General Chemistry.* 3d ed. Boston: Houghton Mifflin, 1990.

Ebinger, Charles K. *Nuclear Power: The Promise of New Technologies.* Washington, D.C.: CSI Studies, 1991.

Edde, Byron. *RADAR: Principles, Technology, Applications.* Englewood Cliffs, NJ: PTR Prentice Hall, 1993.

Edelstein, Herbert A. *Introduction to Data Mining and Knowledge Discovery, Third Edition.* Potomac, MD: Two Crows Corporation, 1999.

Edwardes, Michael. *Playing the Great Game: A Victorian Cold War.* London: Hamish Hamilton, 1975.

Einstein, Albert. *Relativity: The Special and General Theory.* New York: Crown, 1961.

Eisenberg, Dennis, Uri Dan, and Eli Landau. *The Mossad Inside Stories: Israel's Secret Intelligence Service.* New York: Paddington Press, 1978.

Eisenbud, M. *Environmental Radioactivity.* New York: Norton, 1987.

Eisenbud, M., and T. F. Gesell. *Environmental Radioactivity: From Natural, Industrial, and Military Sources.* Academic Press, 1997.

El-Rabbany, Ahmed. *Inroduction to GPS: The Global Positioning System.* Norwood, MA: Artech Publishing, 2002.

Ellis, Richard J. *The Dark Side of the Left: Illiberal Egalitarianism in America.* Lawrence, KS: University Press of Kansas, 1998.

Ellis, Richard. *Encyclopedia of the Sea.* New York: Knopf, 2000.

Ellison, D. Hank. *Handbook of Chemical and Biological Warfare Agents.* Boca Raton, FL: CRC Press, 1999.

Elliston, Jon (introduction). *InTERRORgation: The CIA's Secret Manual on Coercive Questioning,* 2nd edition. San Francisco: AK Press, 1999.

Ellman, Steven J., and John S. Antrobus, eds. *The Mind in Sleep: Psychology and Psychophysiology.* New York: John Wiley & Sons, 1991.

Emerson, Steven, and Brian Duffy. *The Fall of Pan Am 103.* New York: Putnam, 1990.

Emmer, Michele. *The Visual Mind: Art and Mathematics.* Cambridge, MA: MIT Press, 1993.

Emsley, John. *Nature's Building Blocks: An A-Z Guide to the Elements.* Oxford: Oxford University Press, 2002.

Emsley, John. *The Elements.* 3rd ed. New York: Oxford University Press, Inc., 1998.

Engh, T. Abel. *Principles of Metal Refining.* New York: Oxford University Press, 1992.

Engineered Materials Handbook. Metals Park, OH: ASM International, 1988.

Eoghan, Casey. *Digital Evidence and Computer Crime.* New York: Academic Press, 2000.

EPCRA: Emergency Planning and Community Right-to-Know Act. Chicago: American Bar Association Section of Environment, Energy, and Resources, 2002.

Epstein, L.C. *Thinking Physics: Practical Lessons in Critical Thinking.* 2nd ed. San Francisco: Insight Press, 1994.

Epstein, Leon D. *British Politics in the Suez Crisis.* Urbana: University of Illinois Press, 1964.

Eras, Vincent J. M. *Locks and Keys Throughout the Ages.* Schiedam: Interbook International, 1975.

Ernst & Young. "The Economic Contributions of the Biotechnology Industry to the U.S. Economy." *Biotechnology Industry Organization.* 2000.

Eshed, Haggai. *Reuven Shiloah: The Man Behind the Mossad: Secret Diplomacy in the Creation of Israel.* Portland, OR: F. Cass, 1997.

Essenfeld, Bernice, Carol R. Gontang, and Randy Moore. *Biology.* Menlo Park: Addison Wesley, 1996.

Euclid. *Elements.* Translated by Sir Thomas L. Heath. New York: Dover Publishing Co., 1956.

Evans A.M. *An Introduction to Economic Geology and its Environmental Impact.* Blackwell Science, 1997.

Evans, Anthony. *Ore Geology and Industrial Minerals: An Introduction.* Boston: Blackwell Scientific Publications, 1993.

Evans, Brian. *Understanding Digital TV: The Route to HDTV.* New York, NY: IEEE Press, 1995.

Evans, Charles M. *The War of the Aeronauts: A History of Ballooning during the Civil War.* Mechanicsburg, PA: Stackpole Books, 2002.

Evans, Collin. *The Casebook of Forensic Detection: How Science Solved 100 of the World's Most Baffling Crimes.* New York: Wiley, 1996.

Evans, E.A. *Tritium and its Compounds.* New York: Wiley, Inc., 1974.

Eves, Howard Whitley. *Foundations and Fundamental Concepts of Mathematics.* New York: Dover, 1997.

Ewing, Alphonse B. *USA Patriot Act.* Hauppauge, N.Y.: Nova Science Publishing, 2003.

Ewing, Galen W. *Instrumental Methods of Chemical Analysis.* 4th ed. New York: McGraw-Hill Book Company, 1975.

Fah-Chun Cheong. *Internet Agents: Spiders, Wanderers, Brokers, and 'Bots.* Indianapolis, IN: New Riders, 1996.

Fain, Tyrus G., and Katharine C. Plant. *The Intelligence Community: History, Organization, and Issues.* New York: R. R. Bowker, 1977.

Fairchild, D. M. *Ground Water Quality and Agricultural Practices.* Chelsea, MI: Lewis, 1988.

Faith, W.L., Donald Keyes, and Ronald Clark. *Industrial Chemicals.* New York: John Wiley & Sons, 1966.

Falcoff, Mark. *Panama's Canal: What Happens When the United States Gives a Small Country What It Wants.* Washington, D.C.: AEI Press, 1998.

Farson, Stuart, and Catherine J. Matthews. *Criminal Intelligence and Security Intelligence: A Selected Bibliography.* Toronto: Center of Criminology, University of Toronto, 1990.

Feather, Ralph M. et al. *Science Connections.* Columbus, OH: Merrill Publishing Company, 1990.

Feis, Willam B. *Grant's Secret Service: The Intelligence War from Belmont to Appomattox.* Lawrence, KS: University Press of Kansas, 2002.

Feldman, Anthony, and Peter Ford. *Scientists & Inventors.* New York: Facts on File, 1979.

Felix, Antonia. *Condi: The Condoleeza Rice Story.* New York: Newmarket Press, 2002.

Felix, Christopher. *A Short Course in the Secret War.* New York: Dell Books, 1988.

Ferbrache, David. *Germany.* Springer Verlag, 1992.

Ferguson, Amanda, and Nancy L. Stair. *The Attack on U.S. Servicemen at Khobar Towers in Saudi Arabia on June 25, 1996.* New York: Rosen Publishing Group, 2003.

Fermi, Rachel and Esther Samra. *Picturing the Bomb: Photographs from the Secret World of the Manhattan Project.* New York: H.N. Abrams, 1995.

Fewsmith, Joseph. *China Since Tiananmen.* Cambridge University Press, 2001.

Feynman, Leighton, and Sands. *The Feynman Lectures on Physics.* New York: Addison-Wesley, 1989.

Fialka, John J. *War By Other Means: Economic Espionage in America.* New York: W. W. Norton & Company, 1997.

Field, George, and Donald Goldsmith. *The Space Telescope.* Chicago: Contemporary Books, 1989.

Fields, Bernard N., Peter M. Howley, and Diane E. Griffin (eds.). *Virology.* Philadelphia: Lippincott Williams & Wilkins, 2001.

Finn, Elizabeth A. *Pox Americana: Great Smallpox Epidemic of 1775–82.* New York: Hill & Wang, 200.

Finnegan, John Patrick, and Romana Danysh. *Military Intelligence.* Washington, D.C.: Center of Military History, United States Army, 1998.

Finney, Thomas, Demana, and Waits. *Calculus: Graphical, Numerical, Algebraic.* Reading Mass.: Addison Wesley Publishing Co., 1994.

Firschein, Oscar, and Thomas M. Strat. *RADIUS: Image Understanding for Imagery Intelligence.* San Francisco: Morgan Kaufmann Publishers, 1997.

Fischer, Ben B. *At Cold War's End: U.S. Intelligence on the Soviet Union and Eastern Europe,* Washington, D.C.: Center for the Study of Intelligence, 1999.

Fischer, Ben B. *Okhrana: The Paris Operations of the Russian Imperial Police.* Washington, D.C.: Center for the Study of Intelligence, 1997.

Fischetti, Vincent, Richard P. Novick, Joseph J. Ferretti, and Danile A. Portnoy. *Gram-Positive Pathogens.* Washington: American Society for Microbiology Press, 2000.

Fisher, David E. *Fire and Ice: The Greenhouse Effect, Ozone Depletion, and Nuclear Winter.* New York: Harper & Row, 1990.

Fitch, J. Patrick. *Synthetic Aperture RADAR.* West Hanover, MA: Springer-Verlag, 2001.

Fites, Philip, Peter Johnston, and Martin Kratz. *The Computer Virus Crisis.* New York: Van Nostrand Reinhold, 1992.

Fitzgerald, Merni Ingrassia. *The Voice of America.* New York: Dodd, Mead, 1987.

Fleissner, Jennifer. *The Federal Communications Commission.* New York: Chelsea House Publishers, 1992.

Fleming, D. O., and D. L. Hunt. *Biological Safety: Principles and Practices.* 3rd ed. Washington: American Society for Microbiology, 2000.

Fleming, D.O., and D.L. Hunt. *Biological Safety: Principles and Practices,* 3rd ed. Washington: American Society for Microbiology, 2000.

Flint, S.J., et al. *Principles of Virology: Molecular Biology, Pathogenesis, and Control.* Washington: American Society for Microbiology, 1999.

Foot, M.R.D. *SOE: An Outline History of the Special Operations Executive 1940–46.* London: British Broadcasting Corporation, 1984.

Foote, Shelby. *The Civil War—A Narrative.* New York: Vintage Books/Random House, 1986.

Ford, Harold P. *CIA and the Vietnam Policymakers: Three Episodes, 1962–1968.* Washington, D.C.: History Staff, Center for the Study of Intelligence, 1998.

Ford, Harold P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating.* Lanham, MD: University Press of America, 1993.

Foreign and Commonwealth Office Special Review Team. *List of Papers Released From the Previously Retained FCO Archive.* London: LRD, 1994. 2d ed. London: LRD, 1995.

Foreign and Commonwealth Office. *Library and Records Department. Historical Branch. IRD: Origins and Establishment of the Foreign Office Information Research Department, 1946–8.* London: LRD/FCO, 1995.

Forsberg, Randall. *Nonproliferation Primer: Preventing the Spread of Nuclear, Chemical, and Biological Weapons.* Cambridge, MA: MIT Press, 1995.

Forster, Christopher F. *Environmental Biotechnology.* New York: John Wiley & Sons, 1987.

Fowler, C.M.R. *The Solid Earth.* Cambridge: University Press, 1990.

Fox, Nicols. *Spoiled: Why Our Food is Making Us Sick and What We Can Do About It.* New York: Penguin USA, 1998.

Fox, Robert W., and Alan T. McDonald. *Introduction to Fluid Mechanics.* 5th ed. New York: John Wiley & Sons, 1998.

Francis, Frederick. *Wiley Encyclopedia of Food Science and Technology.* New York: Wiley, 1999.

Frank, Benis M. *U.S. Marines in Lebanon, 1982–1984.* Washington, D.C.: U.S. Marine Corps, 1987.

Freedman, Maurice. *Unravelling Enigma: Winning the Code War at Station X.* Barnsley, South Yorkshire, England: Leo Cooper, 2000.

Freeman, R. L. *Telecommunication System Engineering.* New York: Wiley, 1989.

Freeze, R. A., and J. A. Cherry. *Ground Water.* Englewood Cliffs, NJ: Prentice-Hall, 1979.

Freeze, R., and J.Cherry. *Groundwater.* Englewood Cliffs: Prentice-Hall, Inc., 1979.

Freund, John E., and Richard Smith. *Statistics: a First Course.* Englewood Cliffs, NJ: Prentice Hall Inc., 1986.

Fried, Bernard, and Joseph Sherma. *Thin-Layer Chromatography (Chromatographic Science, V. 81).* New York: Marcel Dekker, 1999.

Friedlander, S. K. *Smoke, Dust and Haze: Fundamentals of Aerosol Behavior.* New York: John Wiley & Sons, 1977.

Friedman, J., F. Dill, M. Hayden, and B. McGillivray *Genetics.* Maryland: Williams & Wilkins, Bantam, 1996.

Friend, J. Newton. *Man and the Chemical Elements: An Authentic Account of the Successive Discovery and Utilization of the Elements From the Earliest Times to the Nuclear Age.* 2nd revised ed. New York: Charles Scribner's Sons, 1961.

Frist, W.H. *When Every Moment Counts: What You Need to Know About Bioterrorism from the Senates only Doctor.* Lanham, MD: Rowman & Littlefield, 2002.

Fritz, Sandy, and Jack Brown. *Understanding Germ Warfare (Science Made Accessible).* New York: Warner Books, 2002.

Fritz, W., and J. Moore. *Basics of Physical Stratigraphy and Sedimentology.* New York: John Wiley & Sons, 1988.

Fuller, Buckminster. *Ideas and Integrities.* Toronto: Collier Books, 1963.

Fursenko, Alexandr, and Timothy J. Naftali. *One Hell of a Gamble: Khrushchev, Castro, and Kennedy, 1958–1964.* New York: W. W. Norton and Company, 1998.

Gaddis, John L. *The United States and the Origins of the Cold War.* rev. ed. New York: Columbia University Press, 2000.

Gaddis, John L. *We Now Know: Rethinking Cold War History.* New York: Oxford University Press, 1997.

Gaffney, Timothy, R. *Secret Spy Satellites: America's Eyes in Space.* Berkeley Heights, NJ: Enslow Publishers Inc., 2000.

Gall, Carlotta, and Thomas De Waal. *Chechnya: Calamity in the Caucasus.* New York: New York University Press, 1998.

Gallagher, Thomas Michael. *Assault in Norway: Sabotaging the Nazi Nuclear Bomb.* New York: Harcourt Brace Jovanovich, 1975.

Gann, Ernest Kellogg. *The Black Watch: The Men Who Fly America's Secret Spy Planes.* New York: Random House, 1989.

Ganong, W. F. *Review of Medical Physiology,* 16th ed. Prentice-Hall International, Inc., 1993.

Gardner, Joan F., and Margaret M. Peel. *Introduction to Sterilization and Disinfection.* Melbourne: Churchill Livingstone, 1986.

Gardner, Martin. *Codes, Ciphers, and Secret Writing.* New York: Pocket Books, 1974.

Gardner, Robert. *Crime Lab 101: Experimenting with Crime Detection.* New York: Walker, 1992.

Garrett, L. *The Coming Plague: Newly Emerging Diseases in a World out of Balance.* New York: Penguin Books, 1995.

Gasman, Daniel. *Haeckel's Monism and the Birth of Fascist Ideology.* New York: Peter Lang, 1998.

Gasman, Daniel. *The Scientific Origins of National Socialism: Social Darwinism in Ernst Haeckel and the German Monist League.* London: Macdonald, 1971.

Gates, Robert M. *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War.* New York: Simon and Schuster, 1996.

Gebhardt, James F. *Soviet Special Purpose Forces: An Annotated Bibliography.* Fort Leavenworth, KS: U.S. Army Combined Arms Center, Soviet Army Studies Office, May 1990.

Gelfond, A.O. *Transcendental and Algebraic Numbers.* Dover Publications, 2003.

Gellately, Robert. *The Gestapo and German Society.* Oxford: Oxford University Press, 1991

Gelman, Robert B. and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace.* New York: HarperEdge, 1998.

George, John, and Laird Wilcox. *American Extremists: Militias, Supremacists, Klansmen, Communists, and Others.* Amherst, NY: Prometheus Books, 1996.

Gerson, Allan, and Jerry Adler. *The Price of Terror.* New York: HarperPerennial, 2002.

Gibson, David J. *Methods in Comparative Plant Population Ecology.* Oxford: Oxford University Press, 2002.

Gilbert, Abby L. *A Historical Guide to the U.S. Government.* George T. Kurian, ed. New York and Oxford: Oxford University, 1998.

Gilbert, James L., and John Patrick Finnegan. *U.S. Army Signals Intelligence in World War II: A Documentary History.* Washington, D.C.: U.S. Government Printing Office, 1993.

Gilbert, Martin. *The First World War: A Complete History.* New York: Henry Holt, 1996.

Gilderhus, Mark T. *The Second Century: U.S.-Latin American Relations Since 1889.* Wilmington, DE: Scholarly Resources, 2000.

Gill, Arthur, Steve Krar, and Peter Smid. *Machine Tool Technology Basics.* New York: Industrial Press, 2002.

Gillespie, Angus K. *Twin Towers: The Life of New York City's World Trade Center.* New Brunswick, NJ: Rutgers University Press, 1999.

Gillies, James, and R. Cailliau. *How the Web Was Born: The Story of the World Wide Web.* New York: Oxford University Press, 2000.

Gilligan, Tom. *CIA Life: 10,000 Days with the Agency.* Connecticut: Foreign Intelligence Press, 1991.

Gilmour, Robert S., and Alexis A. Halley. *Who Makes Public Policy? The Struggle for Control Between Congress and the Executive.* Chatham, NJ: Chatham House Publishers, 1994.

Gilpin, Alan. *Dictionary of Fuel Technology.* New York: Philosophical Library, 1969.

Glasston, Samuel and Alexander Sesonske. *Nuclear Reactor Engineering: Vol. 1, Reactor Design Basics.* New York: Chapman & Hall, 1994.

Glelek, Jame. *Chaos: Making a New Science.* New York: Viking Penguin, Inc., 1988.

Glick, B. R., and J. J. Pasternak. *Molecular Biotechnology, Principles and Applications of Recombinant DNA,* 2nd edition. Washington: American Society of Microbiology Press, 1998.

Global Trends 2015: A Dialogue about the Future with Nongovernment Experts. Langley, CA: National Intelligence Council, 2000.

Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence.* Washington: Brassey's, 1996.

Godson, Roy. *United States Intelligence at the Crossroads: Agendas for Reform.* Washington: Brassey's, 1995.

Godwin, Robert. *X-15: The NASA Mission Reports, Incorporating Files from the USAF.* Burlington, Ontario: Apogee Books, 2000.

Göksu, H.Y., M. Oberhofer, and D. Regulla, Eds. *Scientific Dating Methods.* Boston: Kluwer Academic Publishers, 1991.

Gold, Mark and Michael Boyette. *Wonder Drugs: How They Work.* New York: Simon & Schuster, 1987.

Goldreich, Oded. *Foundations of Cryptography: Basic Tools* Cambridge: Cambridge University Press, 2001.

Goldsmith, Robert, and Donald Hayneman, eds. *Tropical Medicine and Parasitology.* Norwalk, CT: 1989.

Goldstein, G., and M. Hersen, eds. *Handbook of Psychological Assessment.* 2nd ed. New York: Pergamon Press, 1990.

Goldstein, Herbert, Charles P. Poole, and John L. Safko. *Classical Mechanics.* 3rd ed. New York: Prentice Hall, 2002.

Goldstein, Martin, and Inge Goldstein. *The Refrigerator and the Universe: Understanding the Laws of Energy.* Harvard University Press, 1993.

Goleniewski, Lillian. *Telecommunication Essentials.* Boston: Addison Wesley Professional, 2001.

Golos, E.B. *Foundations of Euclidean and Non-Euclidean Geometry.* New York: Holt, Rinehart and Winston, 1968.

Goodman and Gilman. *The Pharmacological Basis of Therapeutics.* 6th ed. New York: Macmillan, 1980.

Goodman, H. Maurice. *Basic Medical Endocrinology.* 2nd ed. New York: Raven Press, 1994.

Goodwin, Peter H. *Engineering Projects for Young Scientists.* New York: Franklin Watts, 1987.

Gorbaty, Martin L., John W. Larsen, and Irving Wender, eds. *Coal Science.* New York: Academic Press, 1982.

Gordon, Nathan J., William L. Fleisher, and C. Donald Weinberg. *Effective Interviewing and Interrogation Techniques.* New York: Academic Press, 2001.

Gordievsky, Oleg, and Christopher Andrew. *KGB, The Inside Story of its Foreign Operations from Lenin to Gorbachev.* New York: Harper Collins, 1990.

Gore, Albert. *Department of State and U.S. Information Agency: Accompanying Report of the National Performance Review.* Washington, D.C.: U.S. Government Printing Office, 1993.

Gorman, Martyn L., and R. David Stone. *The Natural History of Moles.* Ithaca, NY: Comstock Publishing Associates, 1990.

Gormley, Dennis. *Dealing with the Threat of Cruise Missiles.* New York: Oxford University Press for the International Institute for Strategic Studies, 2001.

Gosling, F.G. *The Manhattan Project: Science in the Second World War.* U.S. Department of Energy, 1990.

Gottschalk, Jack A. and Brian P. Flanagan. *Jolly Roger With an Uzi: The Rise and Threat of Modern Piracy.* Annapolis: Naval Institute Press, 2000.

Gough, M. *Agent Orange: The Facts.* New York: Perseus Books, 1986.

Gough, W., et al. *Vibrations and Waves.* 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1995.

Goulden, Joseph C. *Korea, the Untold Story of the War.* New York: Times Books, 1982.

Gowar, Norman. *An Invitation to Mathematics.* New York: Oxford University Press, 1979.

Goyer, R.A. "Toxic Effects of Metals." *Casarett and Doull's Toxicology: The Basic Science of Poisons,* 5th edition. New York: McGraw-Hill Companies, Inc., 1996.

Graebner, Norman A., ed. *The National Security: Its Theory and Practice, 1945–1960.* New York: Oxford University, Press, 1986.

Graetzer, Hans G., and David L. Anderson. *The Discovery of Nuclear Fission: A Documentary History.* New York: Van Nostrand Reinhold, 1971. Reprint: Arno Press, 1981.

Graetzer, Hans G., and Larry M. Browning. *The Atomic Bomb: An Annotated Bibliography.* Pasadena: Salem Press, l992.

Grafe, A. *A History of Experimental Virology.* New York: Springer-Verlag, 1991.

Graham, L. *Science in Russia and the Soviet Union.* Cambridge: Cambridge University Press, 1993.

Grant, David, and Robin Harris. *Encyclopedia of Nuclear Magnetic Resonance.* New York: Wiley, 2003.

Graves, Harold N. *On the Short Wave.* New York: Foreign Policy Association, 1941.

Gray, Henry, Lawrence H. Bannister, Martin M. Berry, and Peter L. Williams, eds. *Gray's Anatomy: The Anatomical Basis of Medicine & Surgery.* London: Churchill Livingstone, 1995.

Gray, J. *Man Against Disease-Preventive Medicine.* New York: Oxford University Press, 1979.

Green, Michael. *Bomb Detection Squads.* Mankato, MN: Capstone Press, 1998.

Green, Robert E. *Machinery's Handbook.* 24th ed. New York: Industrial Press, 1992.

Greenwood, N. N. and A. Earnshaw. *Chemistry of the Elements.* New York: Butterworth-Heinemann, 1997.

Gregg, Robert. *International Relations on Film.* Boulder, CO: Lynne Rienner Publishers, 1998.

Gregory, B. *Inventing Reality: Physics as Language.* New York: John Wiley & Sons, 1990.

Greider, William. *Secrets of the Temple: How the Federal Reserve Runs the Country.* New York: Simon and Schuster, 1987.

Gribbin, John. *Q is for Quantum: An Encyclopedia of Particle Physics.* New York: The Free Press, 1998.

Griffith, H. Winter. *Complete Guide to Prescription and Non-Prescription Drugs.* Los Angeles: The Body Press, 1991.

Griffiths, A. et al. *Introduction to Genetic Analysis,* 7th ed. New York, W.H. Freeman and Co., 2000.

Grigg, E.R.N. *The Trail of Invisible Light for X-Strahlen to Radiobiology.* Springfield, IL: Charles C. Thomas, 1965.

Griswold, Terry, and D. M. Giangreco. *Delta, America's Elite Counterterrorist Force.* Osceola, WI: Motorbooks International, 1992.

Grose, Peter. *Gentleman Spy: The Life of Allen Dulles.* Boston: Houghton Mifflin, 1994.

Grose, Peter. *Operation Rollback: America's Secret War Behind the Iron Curtain.* Boston: Houghton-Mifflin, 2000.

Gross, M. L., R. Caprioli, and P. B. Armentrout. *The Encyclopedia of Mass Spectrometry: Ion Chemistry and Theory.* Oxford: Pergamon Press, 2001.

Groves, Donald G. and Lee M. Hunt. *Ocean World Encyclopedia.* New York: McGraw-Hill Book Company, 1980.

Guide to Background Investigations: A Comprehensive Source Directory for Employee Screening and Background Investigations. Tulsa, OK: T.I.S.I., 1998.

Guilbert J.M., and C.F. Park. *The Geology of Ore Deposits.* W.H. Freeman, 1986.

Gullberg, Jan, and Peter Hilton. *Mathematics: From the Birth of Numbers.* W.W. Norton & Company, 1997.

Gundermann, K.D., and F. McCapra. *Chemiluminescence in Organic Chemistry.* New York: Springer-Verlag, 1987.

Gunston, Bill. *The Development of Jet and Turbine Aero Engines.* 2nd ed. New York: Haynes Publishing, 1998.

Guyton, A. C. *Human Physiology and Mechanisms of Disease.* 4th ed. Philadelphia: W.B. Saunders Co., 1987.

Guyton, A.C., and J.E. Hall. *Textbook of Medical Physiology,* 10th ed. New York: W.B. Saunders Company, 2000.

Haass, Richard, and Meghan L. O'Sullivan. *Honey and Vinegar: Incentives, Sanctions, and Foreign Policy.* Washington, D.C.: Brookings Institution Press, 2000.

Haber-Schaim et. al. *Introductory Physical Science.* 5th ed. Englewood Cliffs, N.J.: Prentice-Hall, 1987.

Hafner, Katie, and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet.* New York: Simon & Schuster, 1996.

Hafner, R.S. (Editor). "Transportation, Storage, and Disposal of Radioactive Materials: Presented at the 1999" *Asme Pressure Vessels and Piping Conference.* American Society of Mechanical Engineers, 1990.

Hagen, Robert M., and James Trefil. *Science Matters.* New York: Doubleday, 1991.

Hager, Nicky. *Secret Power.* Nelson, New Zealand: Craig Potton, 1996.

Hahn, Liang-shin. *Complex Numbers and Geometry.* 2nd ed. The Mathematical Association of America, 1996.

Haines, G.K., and R.E. Leggett, eds. *CIA's Analysis of the Soviet Union 1947–1991.* Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 2001.

Halberstam, David. *New York September 11.* New York: PowerHouse Books, 2001.

Haldane, Robert A. *The Hidden War.* New York: St. Martin's, 1978.

Hamblin, W.K., and E.H. Christiansen. *Earth's Dynamic Systems.* 9th ed. Upper Saddle River: Prentice Hall, 2001.

Hammel, Eric M. *The Root: The Marines in Beirut, August 1982-February 1984.* San Diego: Harcourt Brace Jovanovich, 1985.

Hammond, Thomas Taylor, comp. and ed. *Soviet Foreign Relations and World Communism: A Selected, Annotated Bibliography of 7,000 Books in 30 Languages.* Princeton, NJ: Princeton University Press, 1965.

Hamzah, Khidr Ald Al-Abbis, and Jeff Stein. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraq Nuclear and Biological Weapons Agenda.* New York: Scribner, 2002.

Han, Jiawei, and Micheline Kamber. *Data Mining: Concepts and Techniques.* New York: Morgan Kaufmann Publishers, 2000.

Han, M.Y. *The Probable Universe.* Blue Ridge Summit, PA: TAB Books, 1993.

Hancock P. L. and B. J. Skinner, eds. *The Oxford Companion to the Earth.* Oxford: Oxford University Press, 2000.

Handberg, Roger.*Ballistic Missile Defense and the Future of American Security: Agendas, Perceptions, Technology and Policy.* Westport, CT: Praeger,2002.

Haney, Eric L. *Inside Delta Force: The Story of America's Elite Counterterrorist Unit.* New York: Delacorte Press, 2002.

Harden, Victoria Angela. *Rocky Mountain Spotted Fever: History of a Twentieth-Century Disease.* Baltimore: Johns Hopkins University Press, 1990.

Hardy, Anne. *The Epidemic Streets: Infectious Diseases and the Rise of Preventive Medicine, 1956–1900.* New York: Oxford University Press, 1993.

Hardy, M. J. *Sea, Sky, and Stars: An Illustrated History of Grumman Aircraft.* New York: Sterling, 1987.

Hardy, Ralph, Peter Wright, John Kington, and John Gribben. *The Weather Book.* Boston: Little, Brown and Co., 1982.

Hariharan, P. *Basics of Interferometry.* San Diego: Academic Press, 1992.

Harper, David R., and Andrea S. Meyer. *Of Mice, Men, and Microbes: Hantavirus.* San Diego: Academic Press, 1999.

Harper, Richard H.R. *Inside the IMF.* San Diego, CA: Academic Press, 1998.

Harrelson, Leonard. *Lietest: Deception, Truth and the Polygraph.* Ft. Wayne, Indiana: Jonas Publishing, 1998.

Harris, Cyril. *Handbook of Noise Control.* New York: McGraw Hill, 1979.

Harris, Daniel C. *Quantitative Chemical Analysis.* 4th ed. New York: W.H. Freeman & Company, 1995.

Harris, Robert, and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare.* New York: Random House, 2002.

Harris, William R. *Intelligence and National Security: A Bibliography with Selected Annotations. Rev. ed.* Cambridge, MA: Harvard University, Center for International Affairs, 1968.

Harrison, Maureen, and Steve Gilbert. *Landmark Decisions of the United States Supreme Court.* Beverly Hills, CA: Excellent Books, 1991.

Hartcup, Guy. *Camouflage: A History of Concealment and Deception in War.* New York: Scribner's, 1980.

Hartl, Daniel L. *Genetics.* Boston: Jones and Bartlett, 1994.

Hastie, T., et al. *The Elements of Stastical Learning: Data Mining, Inference, and Prediction.* New York: Springer Verlag, 2001.

Hastings, Max. *The Korean War.* New York: Simon and Schuster, 1987.

Haugen, David M. *Biological and Chemical Weapons.* San Diego: Greenhaven Press, 2001.

Hawley, Gessner G. *The Condensed Chemical Dictionary.* New York: Van Nostrand Reinhold Company, 9th edition, 1977.

Hayat, M. Arif. *Microscopy, Immunohistochemistry, and Antigen Retrieval Methods for Light and Electron Microscopy.* New York: Plenum Publishing, 2002.

Haydock, Michael D. *City Under Siege: The Berlin Blockade and Airlift, 1948–1949.* Washington, D.C.: Brasseys, 2000.

Haynes, John Earl, and Harvey Klehr. *Venona: Decoding Soviet Espionage in America.* New Haven, Conn: Yale University Press, 1999.

Heath, R. *Basic Ground-Water Hydrology.* U.S. Geological Survey Water-Supply Paper 2220, 1983.

Hebra, Alexius J. *Measure for Measure: The Story of Imperial, Metric, and Other Units.* Baltimore: Johns Hopkins University Press, 2003.

Hecht, Jeff. *Laser Pioneers.* New York: Academic Press, 1992.

Hecht, Jeff. *Understanding Lasers.* New York: IEEE Press, 1994.

Heiserman, D. L. *Exploring the Chemical Elements and Their Compounds.* Blue Ridge Summit, PA: Tab Publications, 1992.

Helgerson, John. *Getting to Know the President: CIA Briefings of Presidential Candidates,* Washington, DC: Center for Study of Intelligence, CIA, 1995.

Hellemans, Alexander and Bryan Bunch. *The Timetables of Science: A Chronology of the Most Important People and Events in the History of Science.* New York: Simon & Schuster Inc., 1988.

Helms, Harry L. *Shortwave Listening Guidebook: The Complete Guide to Hearing the World.* Solana Beach, CA: High Text Publications, 1993.

Hemond, H. F., and E. J. Fechner. *Chemical Fate and Transport in the Environment.* San Diego: Academic Press, 1994.

Henderson, D.A., and T.V. Inglesby. *Bioterrorism: Guidelines for Medical and Public Health Management.* Chicago: American Medical Association, 2002.

Henderson, Harry. *Privacy in the Information Age.* New York: Facts on File, 1999.

Hendrickson, Robert. *The Ocean Almanac.* Garden City, New York: Doubleday and Company, 1984.

Henne, P. A. *Applied Computational Aerodynamics.* Washington, D.C.: American Institute of Aeronautics and Astronautics, 1990.

Hennessy, Thomas F. *Early Locks and Lockmakers of America.* Des Plaines, IL: Nickerson & Collins Pub. Co., 1976.

Herken, Gregg. *Cardinal Choices: Presidential Science Advising from the Atom Bomb to SDI.* Stanford, CA: Stanford University Press, 2000.

Herman, R. *Fusion: The Search for Endless Energy.* Oxford: Cambridge University Press, 1990.

Hermann, Armin, et al. *History of CERN.* Amsterdam: North-Holland Physics Publishing, 1987.

Herschy, Reginald, and Rhodes Fairbridge, eds. *Encyclopedia of Hydrology and Water Resources.* Boston: Kluwer Academic Publishing, 1998.

Hersh, Burton. *The Old Boys: The American Elite and the Origins of the CIA.* New York: Charles Scribner's Sons, 1992.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis.* Washington, D.C.: Center for the Study of Intelligence, 2000.

Hewitt, Christopher. *Understanding Terrorism in America.* New York: Routledge, 2002.

Hewitt, Steven. *Spying 101: The RCMP's Secret Activities at Canadian Universities.* Toronto: University of Toronto Press, 2002.

Heyman, D.A., J. Achterberg, and J. Laszlo. *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness: A Report on a National Forum on Biodefense.* Washington, DC: Center for Strategic and International Studies, 2002.

Heymann, Philip B. *Terrorism and America: A Commonsense Strategy for a Democratic Society.* Cambridge, Mass.: MIT Press, 1998.

Hidy, G. M. "Aerosols." *Encyclopedia of Physical Science and Technology.* Edited by Robert A. Meyers. San Diego: Academic Press, 1987.

Hillen, John. *Future Visions for U.S. Defense Policy: Four Alternatives Presented as Presidential Speeches.* New York: Council on Foreign Relations, 1998.

Hilliard, Robert L. *The Federal Communications Commission: A Primer.* Boston: Focal Press, 1991.

Hillman, Richard S., John A. Peeler, and Elsa Cardozo da Silva. *Democracy and Human Rights in Latin America.* Westport, CT: Praeger, 2002.

Hinds, William C. *Aerosol Technology : Properties, Behavior, and Measurement of Airborne Particles.* 2nd ed. Hoboken, NJ: Wiley-Interscience,1999.

Hinsley, F. H., et al. *British Intelligences in the Second World War: Its Influence on Strategy and Operations,* Volume Three, Part I. London: Her Majesty's Stationary Office 1984.

Hinsley, F.H. and Alan Stripp, eds. *Codebreakers: The Inside Story of Bletchley Park.* Oxford: Oxford University Press, 2001.

Hinsley, F.H.*British Intelligence in the Second World War.* Cambridge: Cambridge University Press, 1988.

Hiscox, G.D. *Mechanical Movements, Powers, and Devices.* New York: Norman W. Henley Publishing Co., 1927.

History of the Bureau of Engraving and Printing, 1862–1962. Washington, D.C.: Treasury Department, 1964.

Ho, M.W. *Genetic Engineering Dream or Nightmare? The Brave New World of Bad Science and Big Business,* Dublin: Gateway, Gill & Macmillan, 1998.

Hobbs, A. C. *The Construction of Locks.* West Orange, New Jersey: A. Saifer, 1982.

Hobbs, Peter V., and M. Patrick McCormick, eds. *Aerosols and Climate.* Hampton, VA: A. Deepak, 1988.

Hobson, Art. *Physics: Concepts and Connections.* Upper Saddle River, NJ: Prentice Hall, 1994.

Hodgman, Charles D., Editor. *C. R. C. Standard Mathematical Tables.* Cleveland: Chemical Rubber Publishing Co, 1959.

Hodgson, Michael, and Devin Wick. *Basic Essentials: Weather Forecasting.* 2nd ed. Guilford, CT: Globe Pequot Press, 1999.

Hoehling, A.A. *The Great Epidemic.* Boston: Little, Brown and Company, 1961.

Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses.* New York: Van Nostrand Reinhold, 1990.

Hoffman, Lance J., ed. *Building in Big Brother: The Croptographic Policy Debate.* New York: Springer-Verlag, 1995.

Hoffmann, Peter, and Tom Harkin. *Tomorrow's Energy: Hydrogen, Fuel Cells, and Prospects for a Cleaner Planet.* Boston: MIT Press, 2001.

Hogan, Michael H. *A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945–1954.* Cambridge: Cambridge University University Press, 1998.

Hoge, James F., and Gideon Rose. *How Did This Happen?: Terrorism and the New War.* New York: Public Affairs, 2001.

Hogg, R. V., and E. A. Tanis. Probability and Statistical Inference, 6th ed. New Jersey: Prentice Hall, Inc., 2001.

Holder, William G. *Boeing B-52 Stratofortress.* Blue Ridge Summit, PA: AERO, 1988.

Hollien, Harry Francis. *Forensic Voice Identification.* New York: Academic Press, 2001.

Hollien, Harry Francis. *The Acoustics of Crime: The New Science of Forensic Acoustics.* New York: Plenum Press, 1990.

Holloway, David. *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939–1954.* New Haven, Conn.: Yale University Press, 1994.

Holme, David J., and Hazel Peck. *Analytical Biochemistry.* Essex, England: Burnt Mill, Harlow, 1993.

Holmes, Ronald M. *Profiling Violent Crimes: An Investigative Tool.* Newbury Park, England: Sage Publications, 1989.

Holmes, W. J. *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During World War II.* Annapolis, MD: Naval Institute Press, 1979.

Holmes-Siedle, Andrew. *Handbook of Radiation Effects.* New York: Oxford University Press, 1993.

Holober, Frank. *Raiders of the China Coast: CIA Covert Operations during the Korean War (Special Warfare Series).* Annapolis, MD: Naval Institute Press, 1999.

Holton, James R. *An Introduction to Dynamic Meteorology.* 2nd ed. New York: Academic Press, 1979.

Holtzman, Eric, and Alex B. Novikoff. *Cells and Organelles.* Philadelphia: Saunders College Publishing, 1984.

Holum, John R. *Fundamentals of General, Organic and Biological Chemistry.* Wiley and Sons, 1994.

Holzmann, Gerald J., and Bjorn Pehrson. *The Early History of Data Networks.* Los Alamitos, CA: IEEE Computer Society Press, 1995.

Hood, William. *Mole: The True Story of the First Russian Intelligence Officer Recruited by the CIA.* New York: W.W. Norton, 1982.

Hopkins, D.R. *The Greatest Killer: Smallpox in History.* Chicago: University of Chicago Press, 2002.

Hopkins, Donald R. *Princes and Peasants, Smallpox in History* Chicago: The University of Chicago Press, 1983.

Hopkirk, Peter. *The Great Game: The Struggle for Empire in Central Asia.* New York: Kodansha International 1994.

Hopla, C.E., and A.K. Hopla. "Tularemia" *Handbook of Zoonoses.* Boca Raton: CRC Press, 1994.

Hopple, Gerald W., and Bruce W. Watson. *The Military Intelligence Community.* Boulder, CO: Westview Press, 1986.

Horesh, Joshua. *An Iraqi Jew in the Mossad: Memoir of an Israeli Intelligence Officer.* Jefferson, NC: McFarland & Co., 1997.

Horn, Delton E. *DAT: The Complete Guide to Digital Audio Tape.* Blue Ridge Summit, PA: TAB Books, 1991.

Horne, James. *Why We Sleep: The Functions of Sleep in Humans and Other Mammals.* Oxford: Oxford University Press, 1988.

Horowitz, Yigal S., ed. *Thermoluminescence and Thermoluminescent Dosimetry, Vol I and II.* Boca Raton, FL: CRC Press Inc., 1984.

Houde, John. *Crime Lab: A Guide for Nonscientists.* Rolling Bay: Calico Press, 1998.

Houghton, John. *The Physics of Atmospheres.* 3rd ed. Cambridge: Cambridge University Press, 2002.

Houglum, Roger J. *Electronics: Concepts, Applications and History.* 2nd ed. Albany, NY: Delmar Publishers, 1985.

Hoxie, R. Gordon et al. *The Presidency and National Security Policy.* New York: Center for the Study of the Presidency, 1984.

Hubel, David H. *Eye, Brain, and Vision.* New York: Scientific American Library, 1988.

Hudson, John. *The History of Chemistry.* New York: Chapman & Hall, 1992.

Hughes, S. *The Virus: A History of the Concept.* New York: Science History Publications, 1977.

Huisken, Ronald. *The Origin of the Strategic Cruise Missile.* New York: Praeger Publishers, 1981.

Huizenga, John R. *Cold Fusion: The Scientific Fiasco of the Century.* Oxford: Oxford University Press, 1993.

Hunt, Michael H. *Lyndon Johnson's War: America's Cold War Crusade in Vietnam, 1945–1968.* New York: Hill and Wang, 1996.

Ignatius, David. *Agents of Innocence.* New York: W. W. Norton, 1987.

Imagery Intelligence. Washington, D.C.: Department of the Army, 1996.

Immermann, Richard H. *John Foster Dulles and the Diplomacy of the Cold War.* Princeton, NJ: Princeton University Press, 1990.

Incropera, Frank P., and David P. DeWitt. *Fundamentals of Heat and Mass Transfer,* 5th ed. New York: John Wiley & Sons, 2001.

Ingamells, C. O., and Francis F. Pitard. *Applied Geochemical Analysis.* New York, NY: Wiley, 1986.

Inglesby, Thomas V. "Bioterrorist Threats: What the Infectious Disease Community Should Know about Anthrax and Plague." *Emerging Infections 5.* Washington, DC: American Society for Microbiology Press, 2001.

Ingram, Edward. *The Beginning of the Great Game in Asia: 1828–1834.* Oxford: Clarendon, 1979.

INR, Intelligence and Research in the Department of State. Washington, D.C.: Bureau of Intelligence and Research, 1983.

Institute of Medicine. *Assessment of Future Scientific Needs for Live Variola Virus.* Washington, DC: National Academy Press, 1999.

Intelligence Agencies: Personnel Practices at CIA, NSA, and DIA Compared with Those of Other Agencies. Washington, D.C.: General Accounting Office, 1996.

Interrante, Leonard V. *Chemistry of Advanced Materials: An Overview.* Vch Publishing, 1997.

Irvin, Victor D. *Political Assassination: The Strategic Precision Weapon of Choice.* Carlisle Barracks, PA: U.S. Army War College, 2002.

Isselbacher, Kurt J., et al. *Harrison's Principles of Internal Medicine.* New York: McGraw-Hill, 1994.

Isser, Harel. *The House on Garibaldi Street: The First Full Account of the Capture of Adolf Eichmann.* New York: Viking Press, 1975.

Jacobs, George, and Theodore J. Cohen. *The Shortwave Propagation Handbook.* Cowan Publishing Corp., 1970.

Jahn, F., M. Cook, and M. Graham. *Hydrocarbon Exploration and Production. Developments in Petroleum Science.* The Netherlands: Elsevier Science, 2000.

James, I. N. *Introduction to Circulating Atmospheres.* New York: Cambridge University Press, 1994.

James, Lawrence. *Raj: The Making and Unmaking of British India.* New York: St. Martin's Griffin, 1997.

Janseen, Marc, and Nikita Petrov. *Stalin's Loyal Executioner: People's Commissar Nikolai Ezhov 1895–1940.* Palo Alto, CA: Hoover Institution Press, 2002.

Jeffrey-Jones, Rhodri. *The CIA and American Democracy.* New Haven: Yale University Press, 1991.

Jeffreys-Jones, Rhodri, and Christopher M. Andrew. *Eternal Vigilance? 50 Years of the CIA.* Portland, OR: Frank Cass, 1997.

Jeffreys-Jones, Rhodri. *Cloak and Dollar: A History of American Secret Intelligence.* New Haven, CT: Yale University Press, 2002.

Jenkins, Brian Michael. *The Lessons of Beirut: Testimony Before the Long Commission.* Santa Monica, CA: Rand Corporation, 1984.

Jenkins, Dennis R. *Lockheed Secret Projects: Inside the Skunk Works.* St. Paul, MN: MBI Publishing, 2001.

Jenkins, F.A. and H.E. White. *Fundamentals of Optics.* New York: McGraw-Hill, 1976.

Jenner, Edward, Herve Bazin, Andrew Morgan, and Glenise Morgan, trans. *The Eradication of Small Pox: Edward Jenner and the First and Only Eradication of a Human Infectious Disease.* San Diego: Academic Press, 2000.

Jerrard, H. G., and D. B. McNeil. *A Dictionary of Scientific Units: Including Dimensionless Numbers and Scales.* London: Chapman and Hall, 1980.

Joellenbeck, L.M., L.L. Zwanziger, J.S. Durch, et al. *The Anthrax Vaccine: Is It Safe? Does It Work?* Washington, DC: National Academies Press, 2002.

Joesten, Melvin D., David O. Johnston, John T. Netterville, and James L. Wood. *World of Chemistry.* Belmont, CA: Brooks/Cole Publishing Company, 1995.

Johnson, C. K., with M. Smith. *More Than My Share of it All.* Washington, DC: Smithsonian Institution Press, 1985.

Johnson, Eric R. *Servomechanisms.* New York: Prentice-Hall, Inc., 1996.

Johnson, Loch K. *Secret Agencies: U.S. Intelligence in a Hostile World.* New Haven, CT: Yale University Press, 1996.

Johnson, Loch K. *The Central Intelligence Agency: History and Documents.* New York: Oxford University Press, 1989.

Johnson, Robert Erwin. *Guardians of the Sea: History of the United States Coast Guard, 1915 to the Present.* Annapolis: Naval Institute Press, 1987.

Johnson, William, with Jack Maguire. *Who's Stealing Your Business? : How to Identify and Prevent Business Espionage.* New York: AMACOM, American Management Association, 1998.

Joneja, Janice V., and Leonard Bielory. *Understanding Allergy, Sensitivity, and Immunity.* New Brunswick: Rutgers University Press, 1990.

Jones, Dwight V., and Richard F. Shea. *Transistor Audio Amplifiers.* New York: John Wiley & Sons, 1968.

Jones, Joseph. *Stealth Technology.* Blue Ridge Summit, PA: TAB Books, 1994.

Jones, P. M., ed. *Nuclear Power: Policy and Prospects.* New York: John Wiley & Sons, 1987.

Joravsky, D. *The Lysenko Affair.* Cambridge, Massachusetts: Harvard University Press, 1970.

Jorde, L. B., J. C. Carey, M. J. Bamshad, and R. L. White. *Medical Genetics.* 2nd ed. Mosby-Year Book, Inc., 2000.

Jorgensen, E. P., ed. *The Poisoned Well: New Strategies for Groundwater Protection.* Washington, DC: Island Press, 1989.

Jorgenson, Finn. *The Complete Handbook of Magnetic Recording.* 4th ed. New York: McGraw-Hill Professional Book Group, 1995.

Joseph, Robert G., and John F. Reichart. *Deterrence and Defense in a Nuclear, Biological, and Chemical Environment.* Washington, D.C.: Center for Counterproliferation Research, National Defense University, 1999.

Jowett, Garth S., and Victoria O'Donnell. *Propaganda and Persuasion.* Thousand Oaks, CA: Sage Publications, 1999.

Judah, Tim. *Kosovo: War and Revenge.* New Haven, CT: Yale University Press, 2000.

Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence.* Berkeley: University of California Press, 2000.

Julitte, Pierre. *Block 26: Sabotage at Buchenwald.* Garden City, NY: Doubleday, 1971.

Jussim, Daniel. *Drug Tests and Polygraphs.* New York: Julian Messner, A Division of Simon & Schuster, Inc., 1987.

Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms: How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace.* New York: Simon & Schuster, 1996.

Kahn, David. *The Codebreakers: The Story of Secret Writing.* New York: MacMillan Publishing Co., Inc., 1967.

Kahn, David. *Kahn on Codes: Secrets of the New Cryptology.* New York: Macmillan, 1983.

Kahn, David. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* New York: Scribner, 1997.

Kaku, Michio, and Jennifer Trainer. *Nuclear Power, Both Sides: The Best Arguments For and Against the Most Controversial Technology.* New York: W. W. Norton, l982.

Kalpakjian, Serope. *Manufacturing Processes for Engineering Materials.* New York: Addison-Wesley Publishing Company, 1991.

Kalugin, Oleg. *The First Directorate: My 32 Years in Intelligence and Espionage against the West.* New York: St. Martin's Press, 1994.

Karagozian, A. R. "Jet Propulsion." *Encyclopedia of Physical Science and Technology.* Edited by Robert A. Meyers. Orlando, FL: Academic Press, 1987.

Karush, William. *Dictionary of Mathematics.* Webster's New World Printing, 1989.

Katz, Barry M. *Foreign Intelligence: Research and Analysis in the Office of Strategic Services, 1942–1945.* Cambridge, MA: Harvard University Press, 1989.

Katz, Bernard S. C., and Daniel Vencill, eds. *Biographical Dictionary of the United States Secretaries of the Treasury, 1789–1995.* Westport, CT: Greenwood, 1996.

Katz, Samuel M. *Relentless Pursuit: The DSS and the Manhunt for the al-Qaeda Terrorists.* New York: Tom Doherty Associates, 2002.

Kaufman, Charles, et. el. *Network Security: Private Communication in a Public World,* 2nd. ed. Upper Saddle River, NJ: Prentice Hall, 2002.

Kaufman, Yogi. *City at Sea.* Annapolis, MD: Naval Institute Press, 1995.

Kay, Sean. *NATO and the Future of European Security.* Lanham, Maryland: Rowman and Littlefield, 1998.

Keaney, Thomas A. *Strategic Bombers and Conventional Weapons: Airpower Options.* Washington, D.C.: National Defense University Press, 1984.

Keegan, John. *A History of Warfare.* New York: Alfred A. Knopf, 1994.

Keeton, William T., and James L. Gould. *Biological Science.* New York: W.W. Norton and Co., 1993.

Keller, Peter A. *The Cathode-Ray Tube: Technology, History, and Applications.* Palisades Press, 1992.

Kelling, George L. *Broken Windows and Police Discretion.* Washington, D.C.: National Institute of Justice, 1999.

Kelly, John F., and Phillip K, Wearne. *Tainting Evidence: Inside the Scandals at the FBI Crime Lab.* New York: Free Press, 1998.

Kelly, Saul, and Anthony Gorst. *Whitehall and the Suez Crisis.* Portland, OR: Frank Cass, 2000.

Kendrew, J., et al. *The Encyclopedia of Molecular Biology.* Oxford: Blackwell Science Ltd., 1994.

Kennon, Patrick E. *The Twilight of Democracy.* New York: Doubleday, 1995.

Kent, Anthony. *Experimental Low-Temperature Physics.* New York: American Institute of Physics, 1993.

Kent, Sherman. *Strategic Intelligence for American World Policy.* Princeton: Princeton University Press, 1966.

Kessler, Ronald. *Escape from the CIA.* New York: Pocket Books, 1991.

Kessler, Ronald. *Inside the CIA: Revealing the Secrets of the World's Most Powerful Spy Agency.* New York: Pocket Books, 1992.

Kevles, Bettyann Holtzmann. *Medical Imaging in the Twentieth Century.* Rutgers University Press, 1996.

Keynes, Milton. *Handling Laboratory Microorganisms.* Philadelphia: Open University Press, 1991.

Khan, David. *The Codebreakers: The Story of Secret Writing.* New York: Scribner, 1996.

Khan, Munawwar. *Anglo-Afghan Relations, 1798–1878: A Chapter in the Great Game in Central Asia.* Khyber Bazar-Peshawar: University Book Agency, 1963.

Kim, Jin-hyun, and Chung-in Moon. *Post-Cold War, Democratization, and National Intelligence: A Comparative Perspective.* Seoul: Yonsei University Press, 1996.

Kingslake, Rudolph. *A History of the Photographic Lens.* New York: Academic Press, 1989.

Kippenhahn, Rudolf. *Code Breaking: A History and Exploration.* Woodstock, NY: Overlook Press, 1999.

Kirk-Othmer. *Encyclopedia of Chemical Technology.* New York: Wiley, 1991.

Kirkpatrick, Lyman B. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities.* New York: Hill and Wang, 1973.

Kish, John, and David Turns. *International Law and Espionage.* Boston: M. Nijhoff Publishers, 1995.

Kissinger, Henry. *Problems of National Strategy: A Book of Readings.* New York: Praeger, 1965.

Kissinger, Henry. *Years of Renewal.* New York: Simon and Schuster, 1999.

Kissinger, Henry, and Clare Boothe Luce. *White House Years.* Boston: Little, Brown, 1979.

Kittel, Charles. *Introduction to Solid State Physics.* New York: John Wiley & Sons, 1996.

Klaassen, Curtis D. *Casarett and Doull's Toxicology.* 6 th ed. Columbus: McGraw-Hill, Inc., 2001.

Klass, D.L. *Biomass for Renewable Energy, Fuels, and Chemicals.* Academic Press, 1998.

Klein, C. *The Manual of Mineral Science.* 22nd ed. New York: John Wiley & Sons, Inc., 2002.

Klein, Herbert A. *The Science of Measurement.* New York: Dover, 1974.

Klug, William S., and Michael R. Cummings. *Concepts of Genetics.* 5th ed. Upper Saddle River, NJ: Prentice-Hall, Inc., 1997.

Knapp, Rebecca, et al. *Clinical Epidemiology and Biostatistics.* Baltimore: Williams & Wilkins, 1992.

Knezys, Stasys, and Romanas Sedlickas. *The War in Chechnya.* College Station: Texas A&M University Press, 1999.

Knight, Amy. *Beria: Stalin's First Lieutenant.* Princeton, NJ: Princeton University Press, 1996.

Knott, Stephan F. *Secret and Sanctioned-Covert Operations and the American Presidency.* New York: Oxford University Press, 1996.

Kobayashi, G., Patrick R. Murray, Ken Rosenthal, and Michael Pfaller. *Medical Microbiology.* St. Louis, MO: Mosby, 2003.

Koch, A.L. *Bacterial Growth and Form.* Dordrecht: Kluwer Academic Publishers, 2001.

Koch, S., and B.D. Fila. *Our First Line of Defense, Presidential Reflections.* Washington, D.C.: Center for the Study of Intelligence, 1996.

Koehler, T.M. *Anthrax.* Berlin: Springer Verlag, 2002.

Kohler, John O. *Stasi: The Untold Story of the East German Secret Police.* Boulder, Colorado: Westview Press, 1999.

Kondepudi, Dilip, and Ilya Prigogine. *Modern Thermodynamics: From Heat Engines to Dissipative Structures.* New York: John Wiley & Sons, 1998.

Koneman, E., et al., eds. *Color Atlas and Textbook of Diagnostic Microbiology,* 4th ed. Philadelphia: J. B. Lippincott, 1992.

Koneman, Elmer W. *Color Atlas and Textbook of Diagnostic Microbiology.* 4th ed. Philadelphia: J. B. Lippincott, 1992.

Konheim, Alan G. *Cryptography: A Primer.* New York: Wiley, 1981.

Kornbluh, Peter. *Bay of Pigs Declassified: The Secret CIA Report on the Invasion of Cuba.* New York: New Press, 1998.

Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher was Broken, and How It was Read by the Allies in World War Two.* Frederick, MD: University Publications of America, 1984.

Kozlow, Christopher, and John P. Sullivan. *Jane's Facility Security Handbook.* Alexandria, VA: Jane's Information Group, 2000.

Krasner, R.I. *The Microbial Challenge: Human-Microbe Interactions.* Washington: American Society for Microbiology, 2002.

Krauskopf, K.B. *Introduction to Geochemistry.* New York: McGraw Hill, 1995.

Kreis, John F. *Piercing the Fog: Intelligence and Army Air Forces Operations in World War II.* Washington, D.C.: Air Force History and Museums Program, 1996.

Krepon, Michael. *Commercial Observation Satellites and International Security.* New York: St. Martin's Press, 1990.

Krug, R.M., J.S. Flint, L.W. Enquist, V.R. Racaniello, and A.M. Skalka. *Principles of Virology* Washington: American Society for Microbiology, 1999.

Kruse, Warren G., II., and Jay G. Heiser. *Computer Forensics: Incident Response Essentials.* Boston: Addison Wesley Professional, 2001.

Kuhns, Woodrow J. *Assessing the Soviet Threat: The Early Cold War Years.* Washington, D.C. : Center for the Study of Intelligence, 1997.

Kunz, Diane B. *The Economic Diplomacy of the Suez Crisis.* Chapel Hill: University of North Carolina Press, 1991.

Kupperberg, Paul. *Spy Satellites (The Library of Satellites).* New York: Rosen Publishing Group, 2003.

Kurstak, Edouard, ed. *Control of Virus Diseases.* New York: Marcel Dekker, 1993.

Kyle, Keith. *Suez.* New York: St. Martin's Press, 1991.

La Feber, Walter. *America, Russia, and the Cold War.* McGraw-Hill Humanities, 2001.

Lake, Jon. *Jane's How to Fly and Fight in the F-117A Stealth Fighter.* London: HarperCollins Publishers, 1997.

Lance, Simpson L., ed. *Botulinum Neurotoxin and Tetanus Toxin.* San Diego: Academic Press, 1989.

Landau, Alan M., et. al. *U.S. Special Forces: Airborne Rangers, Delta, and U.S. Navy SEALs.* Osceola, WI: MBI, 1999.

Landesman, Linda Young. *Public Health Management of Disasters: The Practical Guide.* Washington, D.C.: American Public Health Association, 2001.

Lanza, Robert P., Robert Langer, and Joseph P. Vacanti. *Principles of Tissue Engineering.* Academic Press, 2000.

Larish, John J. *Electronic Photography.* Blue Ridge Summit, PA: TAB Professional and Reference Books, 2000.

Lashmar, Paul. *Spy Flights of the Cold War.* Great Britain: Sutton Publishing Limited, 1996.

Lasnier, F. and T. Gan Ang. *Photovoltaic Engineering Handbook.* Bristol, England: IOP Publishing, 1990.

Launius, Roger D. *Innovation and the Development of Flight.* College Station: Texas A&M University Press, 1999.

Laurence, Clifford L. *The Laser Book.* Englewood Cliffs, NJ: Prentice Hall, 1986.

Lavoy, Peter R., Scott D. Sagan, and James J. Wirtz. *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons.* Cornell: Cornell University Press, 2001.

Layton, Peggy Diane. *Emergency Food Storage & Survival Handbook: Everything You Need to Know to Keep your Family Safe in a Crisis.* Roseville, CA: Prima Publishing, 2002.

Leary, William M. ed. *The Central Intelligence Agency: History and Documents.* Tuscaloosa, AL: University of Alabama Press, 1984.

Lebow, Eileen F. *A Grandstand Seat: The American Balloon Service in World War I.* Westport, CT: Praeger, 1998.

Lechevalier, Herbert A., and Morris Solotorovsky, eds. *Three Centuries of Microbiology.* Columbus: McGraw-Hill, 1965.

Lederberg, Joshua, and William S. Cohen. *Biological Weapons: Limiting the Threat (BCSIA Studies in International Security).* Boston: MIT Press, 1999.

Ledwidge, Michael S. *Bas Connection.* New York: Simon & Schuster, 2001.

Leffler, Melvyn P. *A Preponderance of Power: National Security, the Truman Administration, and the Cold War.* Stanford, CA: Stanford University Press, 1992.

Legislative Oversight of Intelligence Activities: The U.S. Experience: A Report. Washington, D.C.: U.S. Government Printing Office, 1994.

Lehninger, A.L., D.L. Nelson, and M.M. Cox. *Principles of Biochemistry.* 2nd ed. New York: Worth, 1993.

Leitzel, Jim. *Economics and National Security.* Boulder, CO: Westview Press, 1993.

Lentz, Harris M. *Assassins and Executions: An Encyclopedia of Political Violence, 1865–1986.* Jefferson, NC: McFarland, 1988.

Leonard, Thomas M. *Panama, the Canal, and the United States: A Guide to Issues and References.* Claremont, CA: Regina Books, 1993.

Lerner, K. Lee., and Brenda Wilmoth Lerner. *World of Genetics.* Detroit: Gale Group, 2001.

Lerner, K. Lee., and Brenda Wilmoth Lerner. *World of Microbiology and Immunology.* Detroit: Gale Group, 2002.

Lerner, K. Lee., and Brenda Wilmoth Lerner. *Encyclopedia of Science,* 3rd ed. Detroit: Gale Group, 2003.

Lesser, Ian O. *Countering the New Terrorism.* Santa Monica, CA: RAND, 1999.

Levine, Ira. *Quantum Chemistry.* 4th ed. New Jersey: Prentice Hall, 1991.

Levine, Michael. *Deep Cover: The Inside Story of How DEA Infighting, Incompetence, and Subterfuge Lost Us the Biggest Battle of the Drug War.* New York: Delacorte Press, 1990.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age.* New York: Viking, 2001.

Lewis, Richard J., ed. *Hawley's Condensed Chemical Dictionary.* 13th ed. New York: Van Nostrand Reinhold, 1997.

Libicki, Martin C. *What Is Information Warfare?* Washington, D.C.: National Defense University, 1995.

Library of Congress. Congressional Research Service. *Soviet Intelligence and Security Services.* 2 vols. Washington, DC: GPO, 1972–1975.

Lide, D. R., ed. *CRC Handbook of Chemistry and Physics.* Boca Raton: CRC Press, 2001.

Lieven, Anatol. *Chechnya: Tombstone of Russian Power.* New Haven, CT: Yale University Press, 1998.

Lifton, Robert Jay. *The Nazi Doctors: Medical Killing and the Psychology of Genocide.* New York: Basic Books, 1986.

Lillesand, T.M., and R.W. Kiefer. *Remote Sensing and Image Interpretation,* 3rd ed. New York: John Wiley and Sons, Inc., 1994.

Linacre, E., and B. Geerts. *Climates and Weather Explained.* New York: Routledge, 1997.

Linde, Erik J. G. van de. *Quick Scan of Post 9/11 National Counterterrorism Policymaking and Implementation in Selected European Countries: Research Project for the Netherlands Ministry of Justice.* Santa Monica, CA: RAND Europe, 2002.

Lindsey, Robert. *The Falcon and the Snowman: A True Story of Friendship and Espionage.* London: Jonathan Cape, 1980.

Lisanti, Tom, and Louis Paul. *Film Fatales: Women in Espionage Films and Television, 1962–1973.* Jefferson, NC: McFarland, 2002.

Livingston, M. Stanley, and John P. Blewett. *Particle Accelerators.* New York: McGraw-Hill, 1962.

Local Law Enforcement Responds to Terrorism: Lessons in Prevention in Preparedness. Washington, D.C.: Office of Community Oriented Policing Services, 2002.

London, Barbara, and John Upton. *Photography,* Fifth ed. New York: Harper Collins College Publishers, 1994.

Lord, Carnes. *The Presidency and the Management of National Security.* New York: Free Press, 1988.

Lorenz, Edward N. *The Nature and Theory of the General Circulation of the Atmosphere.* Geneva: World Meteorological Organization, 1967.

Lothes, Robert N., Michael B. Szymanski, and Richard G. Wiley. *Radar Vulnerability to Jamming.* Boston: Artech House, 1990.

Louis, William Roger, and Roger Owen. *Suez 1956: The Crisis and Its Consequences.* New York: Oxford University Press, 1989.

Lovell. Mary S. *Cast No Shadow: The Life of the American Spy Who Changed the Course of World War II.* New York: Pantheon Books, 1992.

Lovett, James E. *Nuclear Materials: Accountability Management Safeguards.* American Nuclear Society, 1974.

Lovins, Amory B., and L. Hunter Lovins. *Brittle Power: Energy Strategy for National Security.* Andover, MA: Brick House Publishing, 1982.

Lovins, Amory B., and L. Hunter Lovins. *Energy/War: Breaking the Nuclear Link.* San Francisco: Friends of the Earth, 1980.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy.* Washington: Congressional Quarterly Press, 2000.

Lowry, Edward D. *Interior Ballistics: How a Gun Converts Chemical Energy into Projectile Motion.* Garden City, NY: Doubleday, 1968.

Loy, James, and Calvin B. Peters. *Understanding Behavior: What Primate Studies Tell Us about Human Behavior.* New York: Oxford University Press, 1991.

Lubbe, J. C. A. van der. *Basic Methods of Cryptography.* New York: Cambridge University Press, 1995.

Lutgens, Frederick K., Edward J. Tarbuck, and Dennis Tasa. *The Atmosphere: An Introduction to Meteorology,* 8th ed. New York: Prentice-Hall, 2000.

Lykken, David T. *A Tremor in the Blood: Uses and Abuses of the Lie Detector.* Reading, Massachusetts: Perseus Books, 1998.

Lynch, Charles T. *Practical Handbook of Materials Science.* Boca Raton, Florida: CRC Press, Inc., 1989.

Macaulay, David, with Neil Ardley. *The New Way Things Work.* Boston: Houghton Mifflin, 1998.

MacDonald, Elizabeth P. *Undercover Girl.* New York: Macmillan, 1947.

MacEachin, Douglas J. *The Final Months of the War with Japan: Signals Intelligence, U.S. Invasion Planning, and the A-Bomb Decision.* Washington, D.C.: History Staff, Center for the Study of Intelligence, 1998.

Madigan, M.M., J. Martinko, and J. Parker. *Brock Biology of Microorganisms,* 8th ed. Upper Saddle River: Prentice-Hall, 2000.

Mahn, W. J. *Academic Laboratory Chemical Hazards Guidebook.* New York: Van Nostrand Rheinhold, 1991.

Major, John. *Prize Possession: The United States and the Panama Canal, 1903–1979.* New York: Cambridge University Press, 1993.

Malcolm, Noel. *Kosovo: A Short History.* New York: New York University Press, 1998.

Mandelbaum, W. Adam. *The Psychic Battlefield: A History of the Military-Occult Complex.* New York: St. Martin's Press, 2000.

Mandeles, Mark David. *The Development of the B-52 and Jet Propulsion: A Case Study in Organizational Innovation.* Maxwell Air Force Base, AL: Air University Press, 1998.

Mandell, Douglas, et al. *Principles and Practice of Infectious Diseases.* New York: Churchill Livingstone, 1995.

Mangano, Joseph, J. *Low level radiation and Immune System Damage: An Atomic Era Legacy.* Boca Raton: Lewis Publishers, 1998.

Mangold, Tom. *Cold Warrior: James Jesus Angleton: The CIA's Master Spy Hunter.* New York: Simon and Schuster, 1991.

Mann, Thomas E. *A Question of Balance: The President, Congress.* Washington, D.C.: Brookings Institution, 1990.

Marchetti, Victor, and John Marks. *The CIA and the Cult of Intelligence.* New York: Alfred A. Knopf, 1974.

Marenches, Count de Alexandre. *The Fourth World War: Diplomacy and Espionage in the Age of Terrorism.* New York: William Morrow and Company, 1992.

Markvart, T., ed. *Solar Electricity.* Chichester, UK: John Wiley, 1994.

Marples, David R., and Marilyn J. Young, eds. *Nuclear Energy and Security in the Former Soviet Union.* Boulder, Colo.: Westview, 1997.

Marshall, Jonathan, Peter Dale Scott, and Jane Haapiseva-Hunter. *The Iran-Contra Connection: Secret Teams and Covert Operations in the Reagan Era.* Boston: South End Press, 1987.

Martin, David C. *Wilderness of Mirrors.* New York: Harper & Row, 1980.

Martin, Shannon E. *Bits, Bytes, and Big Brother: Federal Information Control in the Technological Age.* Westport, CT: Praeger, 1995.

Martini, F. H., et al. Fundamentals of Anatomy and Physiology, 3rd edition. New jersey: Prentice Hall, Inc., 1995.

Matthews, Christopher K., and K. E. Van Holde, eds. *Biochemistry.* 2nd ed. New York: Benjamin/Cummings Publishing Company, 1966.

Mauroni, Albert J. *America's Struggle with Chemical-Biological Warfare.* Westport, CN: Praeger Publishers, 2000.

Mauskopf, Seymour H. *Chemical Sciences in the Modern World.* Pennsylvania: University of Pennsylvania Press, 1993.

Mavis, Paul. *The Espionage Filmography: United States Releases, 1898 through 1999.* Jefferson, NC: McFarland, 2001.

Mawson, Colin. *The Story of Radioactivity.* Englewood Cliffs, NJ: Prentice-Hall, 1969.

Mayer, Kenneth R. *With the Stroke of a Pen: Executive Orders and Presidential Power.* Princeton, NJ: Princeton University Press, 2001.

Mayer, Martin. *The Fed: The Inside Story of the How the World's Most Powerful Financial Institution Drives the Market.* New York: Free Press, 2001.

McAllister, Therese, and Gene Corley. *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations.* Washington, D.C.: Federal Emergency Management Agency, 2002.

McAuliffe, Mary S. *Cuban Missile Crisis 1962.* Washington, D.C.: Center for the Study of Intelligence, 1992.

McCarthy, Dennis V. N., with Philip W. Smith. *Protecting the President: The Inside Story of a Secret Service Agent.* New York: William Morrow, 1985.

McCarthy, Shaun. *Intelligence Services for a Democratic South Africa: Ensuring Parliamentary Control.* London: Research for the Study of Conflict and Terrorism, 1996.

McClintock, P. V. E., D. J. Meredith, and J. K. Wigmore. *Matter at Low Temperatures.* Glasgow: Blackie and Sons, 1984.

McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions, Fourth Edition.* Emeryville, CA: McGraw-Hill Osborne Media, 2003.

McCormick, Anita Louise. *Shortwave Radio Listening for Beginners.* Blue Ridge Summit, PA: TAB Books, 1993.

McCullough, John P., and Donald W. Scott, eds. *Experimental Thermodynamics.* New York: Plenum Press, 1968.

McDougall, Walter. *The Heavens and the Earth: A Political History of the Space Race.* Baltimore: Johns Hopkins University Press, 1997.

McIntosh, Elizabeth P. *Sisterhood of Spies: The Women of the OSS.* Annapolis, MD: Naval Institute Press, 1998.

McKinley, James. *Assassination in America.* New York: Harper & Row, 1977.

McMahon, Rober. *The Cold War on the Periphery.* New York, Columbia University Press 1994.

McNeil, Ian. *An Encyclopaedia of the History of Technology.* New York: Routledge, 1996.

McNeill, Robert. *Understanding the Weather.* Las Vegas: Arbor Publishers, 1991.

Mearna, J., and W.C. Koller, eds. *Parkinson's Disease and Parkinsonism in the Elderly.* New York: Cambridge University Press, 2000.

Medvedev, Zhores. *The Legacy of Chernobyl.* New York: W. W. Norton & Company, 1990.

Melanson, Philip H. *The Politics of Protection: The U.S. Secret Service in the Terrorist Age.* New York: Praeger, 1984.

Melton, H. Keith. *CIA Special Weapons and Equipment: Spy Devices of the Cold War.* New York: Sterling Publishing, 1993.

Melton, H. Keith. *OSS Special Weapons and Equipment: Spy Devices of World War Two.* New York: Sterling Publishing, 1991.

Melton, H. Keith. *The Ultimate Spy Book.* London & New York: Dorling Kindersley, Ltd., 1996.

Mendez, A., and J. Mendez. *Spy Dust: Two Masters of Disguise Reveal the Tools and Operations That Helped Win the Cold War.* New York: Atria Books, 2002.

Mendez, Antonio J. *The Master of Disguise: My Secret Life in the CIA.* New York: Morrow, 1999.

Menges, Constantine Christopher. *Inside the National Security Council: The True Story of the Making and Unmaking of Reagan's Foreign Policy.* New York: Simon and Schuster, 1988.

Merck Manual of Diagnosis and Therapy, 17th edition. Edited by Mark H. Beers, and Robert Berkow. Whitehouse Station, NJ: Merck Research Laboratories, 1999.

Meriam, J.L., and L.G. Kraige. *Engineering Mechanics, Dynamics.* 5th ed. New York: John Wiley & Sons, 2002.

Mertz, L. *Recent Advances and Issues in Biology.* Phoenix, Arizona: Oryx Press, 2000.

Merzbacher, E. *Quantum Mechanics.* New York: John Wiley & Sons, 1997.

Meyer, Carl H., and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security.* New York: John Wiley & Sons 1982.

Meyer, Cord. *Facing Reality: From World Federalism to the CIA.* New York: Harper & Row, 1980.

Meyer, Henry Cord. *Airshipmen, Businessmen and Politics 1890–1940.* Washington DC: Smithsonian Institution Press, 1991.

Meyer, Karl Ernest, and Shareen Blair Brysac. *Tournament of Shadows: The Great Game and the Race for Empire in Central Asia.* Washington, D.C.: Counterpoint, 1999.

Meyers, Robert A. *Encyclopedia of Analytical Chemistry: Applications, Theory and Instrumentation.* New York: John Wiley & Sons, 2000.

Meyers, Robert A., *Encyclopedia of Physics Science and Technology.* New York, NY: Academic Press, Inc., 1992.

Michaels, Patrick J. *Sound and Fury: The Science and Politics of Global Warming.* Washington D. C.: Cato Institute, 1992.

Michel, Lou and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing.* New York: Regan Books, 2001.

Micklos, David, A., and Greg A. Freyer. *DNA Science, A First Course in Recombinant DNA Technology.* United States: Cold Spring Harbor Laboratory Press and Carolina Biological Supply Company, 1990.

Milano, James V. *Soldiers, Spies and the Rat Line: America's Undeclared War against the Soviets.* Washington: Brassey's, 1995.

Miller, A. Ray. *The Cryptographic Mathematics of Enigma.* Ft. Meade, MD: National Security Agency, 2001.

Miller, E. Willard, and Ruby Miller. *Environmental Hazards: Toxic Waste and Hazardous Material: A Reference Handbook.* Santa Barbara, Calif.: ABC-CLIO, 1991.

Miller, Jay. *Lockheed Martin's Skunk Works.* North Branch, MN: Specialty Press, 1995.

Miller, Nathan. *Spying for America: The Hidden History of U.S. Intelligence.* New York: Paragon House, 1989.

Miller, Roger G. *To Save a City: The Berlin Airlift, 1948–1949.* Seattle, WA: University Press of the Pacific, 2002.

Mitrokhin, Vasily, ed. *KGB Lexicon: The Soviet Intelligence Officer's Handbook.* London: Frank Cass, 2002.

Mitrovich, Gregory. *Undermining the Kremlin: America's Strategy to Subert the Soviet Bloc.* Ithaca, NY: Cornell, 2000.

Mitton, Simon P., ed. *The Cambridge Encyclopedia of Astronomy.* Cambridge: Cambridge University Press, 1977.

Modeling and Simulation: Linking Entertainment and Defense. Washington, D.C.: National Academy Press, 1997.

Mollin, Richard A. *An Introduction to Cryptography.* New York: Chapman & Hall, 2001.

Money Factory. Washington, D.C.: Bureau of Engraving and Printing, 1993.

Montagu, Ewen. *Man Who Never Was.* London: Globe Pequot Press,1997.

Montague, Ludwell Lee. *General Walter Bedell Smith as Director of Central Intelligence.* University Park, PA: The Pennsylvania State University Press, 1992.

Montplaisir, Jacques, and Roger Godbout, eds. *Sleep and Biological Rhythms: Basic Mechanisms and Applications to Psychiatry.* New York: Oxford University Press, 1990.

Moore, David, and George McCabe. *Introduction to the Practice of Statistics.* New York: W. H. Freeman, 1989.

Moore, Jim. *Very Special Agents: The Inside Story of America's Most Controversial Law Enforcement Agency—The Bureau of Alcohol, Tobacco, and Firearms.* Urbana: University of Illinois, 2001.

Moore, John, and Nicholas D. Spencer. *Encyclopedia of Chemical Physics and Physical Chemistry.* Washington, D.C.: Institute of Physics, 2001.

Moran, Joseph M., and Michael D. Morgan. *Essentials of Atmosphere and Weather.* New York: Macmillan Publishing Company, 1994.

Morehouse, David. *Psychic Warrior: Inside the CIA's Stargate Program: The True Story of a Soldier's Espionage and Awakening.* New York: St. Martin's Press, 1996.

Morgan, Ted. *A Covert Life: Jay Lovestone: Communist, Anti-Communist, and Spymaster.* New York: Random House, 1999.

Moriarty, Laura J., and David L. Carter. *Criminal Justice Technology in the 21st Century.* Springfield, IL: Charles C. Thomas, 1998.

Motto, Carmine J. *In Crime's Way: A Generation of U.S. Secret Service Adventures.* Boca Raton, FL: CRC Press, 2000.

Mould, R. F. *Chernobyl Record: The Definitive History of the Chernobyl Catastrophe.* Bristol, England: Institute of Physics Publishing, 2000.

Moyar, M. *Phoenix and the Birds of Prey: The CIA's Secret Campaign to Destroy the Viet Cong.* Annapolis, MD: Naval Institute Press, 1997.

Mulhall, Douglas. *Our Molecular Future: How Nanotechnology, Robotics, Genetics, and Artificial Intelligence Will Change Our World.* Amherst, NY: Prometheus Books, 2002.

Mulligan, Geoff. *Removing the Spam: Email Processing and Filtering.* Addison-Wesley, 1999.

Munk W., P. Worcester, and C. Wunsch. *Ocean Acoustic Tomography.* Cambridge: Cambridge University Press, 1995.

Munson, Bruce, et al. *Fundamentals of Mechanics.* 4th ed. New York: John Wiley and Sons, 2002.

Murphy, Christine. *The Vaccine Dilemma.* New York: Lantern Books, 2000.

Murphy, David E., Sergei A. Kondrashev, and George Bailey. *Battleground Berlin: CIA vs. KGB in the Cold War.* New Haven, CT: Yale University Press, 1997.

Murphy, Douglas, B. *Fundamentals of Light Microscopy and Electronic Imaging.* New York: Wiley-Liss, 2001.

Murray, John, James H. Murray, and Barnet Resnick. *A Guide to Taser Technology: Stunguns, Lies, and Videotape.* Dana Point: Whitewater Press, 1997.

Murray, Raymond L. *Nuclear Energy.* 3rd ed. New York: Pergamon Press, l988.

Murray, Williamson, and Allan Reed Millett. *Military Innovation in the Interwar Period.* New York: Cambridge University Press, 1996.

Musciano, Walter A. *Warbirds of the Sea: A History of Aircraft Carriers and Carrier-Based Aircraft.* Atglen, PA: Schiffer Publishing, 1994.

Musicant, Ivan. *The Banana Wars: A History of United States Military Intervention in Latin America from the Spanish-American War to the Invasion of Panama.* New York: Macmillan, 1990.

Mylroie, Laurie. *Study of Revenge: The First World Trade Center Attack and Saddam Hussein's War Against America.* Washington, D.C.: AEI Press, 2001.

Nanavati, Samir, Michael Thieme, and Raj. Nanavati. *Biometrics: Identity Verification in a Networked World.* New York: Wiley and Sons, 2002.

Nataro, J.P., M.J. Blaser, and S. Cunningham-Rundles. *Persistent Bacterial Infections.* Washington: American Society for Microbiology, 2000.

Nathan, James. *Anatomy of the Cuban Missile Crisis.* Westport, CT: Greenwood Press, 2001.

National Academy of Sciences. *Veterans and Agent Orange: Health Effects of Herbicides Used in Vietnam.* Washington, DC: National Academy Press, 1994.

National Communications System for Emergency Response Personnel. Washington, D.C.: Government Printing Office, 2001.

National Communications System, 1963–1998: 35th Anniversary. Arlington, VA: National Communications System, 1998.

National Infrastructure Protection Center (NIPC): A Public-Private Partnership to Protect America's Critical Infrastructures. Washington, D.C.: U.S. Department of Justice, 2002.

National Research Council, Computer Science and Telecommunications Board. *Cyber Security Today and Tommorrow: Pay Now or Pay Later.* Washington, DC: The National Academies Press, 2002.

National Security: The Use of Presidential Directives to Make and Implement United States Policy: Report to the Chairman, Committee on Government Operations, House of Representatives. Washington, D.C.: Government Printing Office, 1988.

National Transportation Strategic Research Plan. Washington, D.C.: National Science and Technology Council, 2000.

Naval Criminal Investigative Service: To Protect and Serve. Washington, D.C.: U.S. Department of the Navy, 1994.

Navarra, John G. *Atmosphere, Weather and Climate.* Philadelphia: W.B. Saunders Co., 1979.

Naveh, Ben-Zin and Azrid Lorber, eds. *Theater Ballistic Missile Defense.* Reston, VA: American Institute of Aeronautics and Astronautics, 2001.

Naylor, R.T. *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy.* Ithaca, NY: Cornell University, 2002.

Nelson, K.E., C.M. Williams, and N.M.H. Graham. *Infectious Disease Epidemiology: Theory and Practice.* Gaithersburg: Aspen Publishers, 2001.

Nelson, Robert A. *SI: The International System of Units.* Stony Brook, N.Y.: American Association of Physics Teachers, 1982.

Neustaedter, Randall. *The Vaccine Guide: Risks and Benefits for Children and Adults.* Berkeley: North Atlantic Books, 2002.

Newman, Elizabeth L. *Security Clearance Law and Procedure.* Arlington, VA: Dewey Publications, 1998.

Newton, David E. *Encyclopedia of Cryptology.* Santa Barbara, CA: ABC-CLIO, 1997.

Newton, David E. *Particle Accelerators: From the Cyclotron to the Superconducting Super Collider.* New York: Franklin Watts, 1989.

Nickell, Joe, and John F. Fischer. *Crime Science: Methods of Forensic Detection.* Lexington: University Press of Kentucky, 1999.

Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Simmons. *Public and Private Applications of Video Surveillance and Biometric Technologies.* Sacramento, CA: California Research Bureau, California Public Library, 2002.

Noor, Ahmed Khairy, and Samuel L. Venneri. *Future Aeronautical and Space Systems.* Reston, VA: American Institute of Aeronautics and Astronautics, 1997.

Notton, John. "The Use of Technology in Policing the City of London," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed. 1998.

Nuclear Power, Nuclear Fuel Cycle and Waste Management, Part C: Status and Trends, 1993. Lanham, MD: UNIPUB, 1993.

Nuclear Safety: The Defense Nuclear Facilities Safety Board's First Year of Operation: Report to Congressional Requesters. Washington, D.C.: General Accounting Office, 1991.

Nussbaum, R. L., R. R. McInnes, and H. F. Willard. *Thompson and Thompson Genetics in Medicine, Sixth Edition.* Philadelphia, PA: Saunders, 2001.

Nutter, John Jacob. *The CIA's Black Ops: Covert Action, Foreign Policy, and Democracy.* Amherst, NY: Prometheus Books, 2000.

Ojeda, Auriana. *Drug Trafficking.* San Diego, CA: Greenhaven Press, 2002.

Olah, George A., ed. *Chemistry of Energetic Materials.* San Diego: Academic Press, 1991.

Olin, Harold B. *Construction; Principles, Materials and Methods.* Danville, Ill.: Interstate Printers and Publishers, 1980.

Olmstead, A. T. *History of the Persian Empire and the Ancient MidEast.* Chicago: University of Chicago Press, 1959.

One Nation: America Remembers September 11, 2001. Boston: Little, Brown, 2001.

O'Neil, Maryadele J. *Merck Index: An Encyclopedia of Chemicals, Drugs, & Biologicals.* 13th ed. Whitehouse Station, NJ: Merck & Co., 2001.

Operation DISA: A Continuing Evolution. Arlington, VA: Defense Information Systems Agency, 1996.

Optical Document Security. Boston: Artech House, 1998.

Orphan, R. C. *A Study of Applying the Atmospheric Release Advisory Capability to Nuclear Power Plants.* Springfield, VA: Department of Energy, 1978.

Osborn, Shane, and Malcolm McConnell. *Born to Fly: The Untold Story of the Downed American Reconnaissance Plane.* New York: Broadway Books, 2001.

Ostmann, Robert. *Acid Rain: A Plague Upon the Waters.* Minneapolis: Dillon, 1982.

Ostrander, Sheila, and Lynn Schroeder. *Psychic Discoveries Behind the Iron Curtain.* Englewood Cliffs, NJ: Prentice-Hall, 1970.

O'Toole, G. J. A. *Honorable Treachery: A History of Intelligence, Espionage, and Covert Action from the American Revolution to the CIA.* New York: Atlantic Monthly Press, 1991.

O'Toole, G. J. A. *The Encyclopedia of American Intelligence and Espionage.* New York: Facts on File, 1988.

Ottis, Sherri Greene. *Silent Heroes: Downed Airmen and the French Underground.* Lexington, KY: University of Kentucky Press, 2001.

Ousby, Ian. *Occupation.* Lanham, MD: Cooper Square Press, 2000.

Owen, David. *Hidden Secrets.* Buffalo, NY: Firefly Books, 2002.

Pace, Steve. *Lockheed Skunk Works.* Osceola, WI: Motorbooks International, 1992.

Packard, Wyman H. *A Century of U.S. Naval Intelligence.* Washington, D.C.: Naval Historical Center, 1996.

Pagana, K.D., *Mosby's Manual of Diagnostic and Laboratory Tests.* St. Louis: Mosby, Inc., 1998.

Paglin, Max D., editor. *A Legislative History of the Communications Act of 1934.* New York: Oxford University Press, 1990.

Park, William. *Defending the West: A History of NATO.* Brighton: Wheatsheaf, 1986.

Parker, James E. *Codename Mule: Fighting the Secret War in Laos for the CIA.* Annapolis, MD: Naval Institute Press, 1995.

Parrish, Michael. *Soviet Security and Intelligence Organizations, 1917–1990: A Biographical Dictionary and Review of Literature in English.* Westport, CT: Greenwood, 1991.

Parrish, Michael. *The Lesser Terror: Soviet State Security, 1939–1953.* Westport, CT: Praeger, 1996.

Patrick, Dale R. and Stephen W. Fardo. *Understanding Electricity and Electronics.* Upper Saddle River, NJ: Prentice Hall, 1989.

Pedlow G.W., and Welzenbach, D.E. *The CIA and the U-2 Program.* Washington, D.C.: History Staff, Center for the Study of Intelligence, 1998.

Peebles, Curtis. *The CORONA Project.* Annapolis: Naval Institute Press, 1997.

Peebles, Curtis. *Shadow Flights: America's Secret Air War Against the Soviet Union.* Novato, CA: Presidio, 2000.

Peebles, Curtis. *The Moby Dick Project: Reconnaissance Balloons over Russia.* Washington, D.C.: Smithsonian Institution Press, 1991.

Peierls, R. E. *Atomic History.* New York: Springer-Verlag, 1997.

Permissible Dose: A History of Radiation Protection in the Twentieth Century. Berkeley: University of California Press, 2000.

Persico, Joseph E. *Casey: From the OSS to the CIA.* New York: Viking Penguin, 1990.

Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage.* New York: Random House, 2001.

Petersen, Julie K. *Understanding Surveillance Technologies: Spy Devices, their Origins & Applications.* Boca Raton, FL : CRC Press, 2001.

Peterson, M. N. A. *Initial Reports of the Deep Sea Drilling Project II.* Washington: Government Printing Office, 1970.

Petit, Michael. *Peacekeepers at War: A Marine's Account of the Beirut Catastrophe.* Boston: Faber and Faber, 1986.

Pforzheimer, Walter, ed. *Bibliography of Intelligence Literature: A Critical and Annotated Bibliography of Open-Source Intelligence Literature. 8th ed.* Washington, DC: Defense Intelligence College, 1985.

Phillips, Bill. *The Complete Book of Locks and Locksmithing.* New York: McGraw-Hill, 1995.

Phillips, David Atlee. *The Night Watch: 25 Years of Peculiar Service.* New York: Atheneum, 1977.

Phillips, David Atlee. *Careers in Secret Operations: How to Be a Federal Intelligence Officer.* Frederick, MD: University Publications of America, 1984.

Physicians Desk Reference 2003 with Physicians Desk Reference Family Guide. Montvale, NJ: Medical Economics, 2002.

Pincher, Chapman. *The Secret Offensive.* New York: St. Martin's, 1985.

Pincher, Chapman. *The Spycatcher Affair.* New York: St. Martin's Press, 1988.

Pinck, D.C., G.M.T. Jones, and C.T. Pinck. *Stalking the History of the Office of Strategic Services: An OSS Bibliography.* Boston: The OSS/Donovan Press, 2000.

Piresein, Robert William.*The Voice of America: A History of the International Broadcasting Activities of the United States Government, 1940–1962.* New York: Arno Press, 1979.

Plischke, Elmer. *U.S. Department of State: A Reference History.* Westport, CT: Greenwood Press, 1999.

Pocock, Chris. *Dragon Lady: The History of the U-2 Spyplane.* Shrewsbury, UK: Airlife Publishing, 1989.

Politkovskaia, Anna. *A Dirty War: A Russian Reporter in Chechnya.* London: Harvill, 2001.

Pollock, David A. *Methods of Electronic Audio Surveillance.* Springfield, IL: Thomas, 1973.

Polmar, Norman. *The Naval Institute Guide to the Ships and Aircraft of the U.S. Fleet.* Annapolis, MD: Naval Institute Press, 1993.

Polmar, Norman, and Thomas B. Allen. *Spy Book: The Encyclopedia of Espionage.* New York: Random House, 1997.

Poolos, J. *Nerve Gas Attack on the Tokyo Subway.* Rosen Publishing Group Inc., 2002.

Porch, Douglas. *The French Secret Services: From the Dreyfus Affair to the Gulf War.* New York: Farrar, Straus & Giroux, 1995.

Porter, Roy, and Marilyn Ogilvie, consultant editors. *The Biographical Dictionary of Scientists.* New York: Oxford University Press, 2000.

Porter, Ted, and Dorothy Ross, eds. *The Cambridge History of Science: Volume 7, The Modern Social Sciences.* Cambridge: Cambridge University Press, 2003.

Pottier, John. *Anthropology of Food: The Social Dynamics of Food Security.* Oxford: Polity Press, 1999.

Powell, Colin L., and Joseph E. Persico. *My American Journey.* New York: Ballantine Books, 1996.

Power, Samantha. *A Problem from Hell: America in the Age of Genocide.* New York: Basic Books, 2002.

Powers, Thomas. *The Man Who Kept the Secrets: Richard Helms and the CIA.* New York: Alfred A. Knopf, 1979.

Prados, John. *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II.* New York: Random House, 1995.

Prados, John. *Keepers of the Keys: A History of the National Security Council from Truman to Bush.* New York: William Morrow & Company, Inc., 1991.

Prados, John. *Lost Crusader: The Secret Wars of CIA Director William Colby.* New York: Oxford University Press, 2003.

Prados, John. *Presidents' Secret Wars: CIA and Pentagon Covert Operations from World War II through Iranscam.* New York: William Morrow, Co., 1986.

Prados, John. *The Soviet Estimate: U.S. Intelligence Analysis and Russian Military Strength.* New York: Dial Press, 1982.

Prange, Gordon W. *At Dawn We Slept: The Untold Story of Pearl Harbor.* New York: McGraw-Hill, 1981.

Prescott, L., J. Harley, and D. Klein. *Microbiology* 5th ed. New York: McGraw-Hill, 2002.

Press, Frank and Raymond Siever. *Understanding Earth.* New York: W. H. Freeman and Company, 2000.

Preston, Anthony. *Carriers.* New York: Gallery Books, 1993.

Preston, Edmund. *FAA Historical Chronology: Civil Aviation and the Federal Government, 1926–1996.* Washington: DOT/FAA, 1998.

Preston, R. *The Demon in the Freezer.* New York: Random House, 2002.

Preston, Richard. *The Demon in the Freezer: A True Story.* New York: Random House, 2002.

Price, Alfred. *War in the Fourth Dimension: U.S. Electronic Warfare, from the Vietnam War to the Present.* London: Greenhill, 2001.

Primrose, S.P. *Principles of Genome Analysis.* Oxford: Blackwell, 1995.

Principal Officers of the Department of State and United States Chiefs of Mission, 1778–1990. Washington, D.C.: U.S. Department of State, 1991.

Pritchard, Michael, and Douglas St. Denny. *Spy Camera: A Century of Detective and Subminiature Cameras.* London: Classic Collections, 1993.

Proakis, John G. *Digital Communications.* New York: McGraw-Hill, 2001.

Purcell, William P. "Benzene." *Kirk-Othmer Encyclopedia of Chemical Technology.* 4th ed. Suppl. New York: John Wiley & Sons, 1998.

Rabilloud, Thierry. *Proteome Research: Two-Dimensional Gel Electrophoresis and Identification Methods (Principles and Practice).* Berlin: Springer Verlag, 2000.

Ranelagh, John. *The Agency: The Rise and Decline of the CIA.* New York: Simon & Schuster, 1987.

Record, Jeffrey. *Making War, Thinking History: Munich, Vietnam, and Presidential Uses of Force from Korea to Kosovo.* Annapolis, MD: Naval Institute Press, 2002.

Reeve, Simon. *The New Jackals: Ramzi Yousef, Osama bin Laden, and the Future of Terrorism.* Boston: Northeastern University Press, 1999.

Rehnquist, William H. *All the Laws But One: Civil Liberties in Wartime.* New York: Alfred A. Knopf, 1998.

Reisman, W. Michael, and James E. Baker. *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law.* New Haven, CT: Yale University Press, 1992.

Reist, Parker C. *Introduction to Aerosol Science.* New York: Macmillan, 1989.

Rhodes, Richard. *Dark Sun: The Making of the Hydrogen Bomb (Sloan Technology Series).* Simon & Schuster, 1995.

Rich, Ben and Leo Janos. *Skunk Works.* New York: Bantam, 1994.

Richelson, Jeffrey T. *A Century of Spies: Intelligence in the Twentieth Century.* New York: Oxford University Press, 1995.

Richelson, Jeffrey T. *The U.S. Intelligence Community,* fourth edition. Boulder, CO: Westview Press, 1999.

Richelson, Jeffrey T. *The Wizards of Langley.* Boulder, Colo.: Westview, 2001.

Richelson, Jeffrey. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries.* Boston: Unwin Hyman, 1990.

Richman, D. D., and R. J. Whitley. *Clinical Virology.* 2nd ed. Washington: American Society for Microbiology, 2002.

Ridgway, Matthew B. *The Korean War: How We Met the Challenge; How All-Out Asian War Was Averted; Why MacArthur Was Dismissed; Why Today's War Objectives Must Be Limited.* Garden City, NY: Doubleday, 1967.

Riebling, Mark. *Wedge: The Secret War Between the FBI and CIA.* New York: Alfred A. Knopf, 1994.

Rifkin, J. *The Biotech Century.* Putnam Publishing Group, 1998.

Rihaczek, August W., and Stephen J. Hershkowitz. *Theory and Practice of Radar Target Identification.* Boston: Artech House, 2000.

Riley, Kevin Jack, and Bruce Hoffman. *Domestic Terrorism: A National Assessment of State and Local Preparedness.* Santa Monica, CA: RAND Corporation, 1995.

Riley, Kevin Jack. *Crack, Powder Cocaine, and Heroin: Drug Purchase and Use Patterns in Six U.S. Cities.* Washington, D.C.: National Institute of Justice, 1998.

Rimoin, David L. *Emery and Rimoin's Principles and Practice of Medical Genetics.* London; New York: Churchill Livingstone, 2002.

Ripley, Randall B., and James M. Lindsay. *U.S. Foreign Policy After the Cold War.* Pittsburgh: University of Pittsburgh Press, 1997.

Rivers, Gayle, and James Hudson. *The Teheran Contract.* Garden City: New York: Doubleday & Company, 1981.

Robarge, David. *Intelligence in the War for Independence.* Washington, D.C.: Center for the Study of Intelligence, 1997.

Roberts, Brad. *Biological Weapons: Weapons of the Future?* Washington, D.C.: Center for Strategic and International Studies, 1993.

Roberts, Brad. *U.S. Foreign Policy After the Cold War.* Cambridge, MA: MIT Press, 1992.

Robertson, Kenneth G. "The Study of Intelligence in the United States." *Comparing Foreign Intelligence: The U.S., the USSR, the U.K. & the Third World.* R. Godson, ed. Washington, DC: Pergamon-Brassey's, 1988.

Rocca, Raymond G., and John J. Dziak. *Bibliography on Soviet Intelligence and Security Services.* Boulder, CO: Westview, 1985.

Rogers, Paul. *Political Violence and Asymmetric Warfare.* (U.S.-European Forum Paper) Washington: Brookings Institution, 2001.

Roit, I.M. *Roit's Essential Immunology.* Oxford: Blackwell Science Ltd., 1997.

Roleff, Tamara. ed. *The Atom Bomb.* San Diego, CA: Greenhaven Press, 2000.

Roosevelt, Archibald. *For Lust of Knowing: Memoirs of an Intelligence Officer.* Boston: Little, Brown, 1988.

Roosevelt, Kermit. *Countercoup: The Struggle for the Control of Iran.* New York: McGraw-Hill Book Co., 1979.

Rose, N.R. *Manual of Clinical Laboratory Immunology,* 4th ed. Washington: American Society for Microbiology, 2002.

Rose, P.K. *Black Dispatches: Black American Contributions to Union Intelligence during the Civil War.* Washington, D.C.: Center for Study of Intelligence, 1999.

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America.* New York: Random House, 2000.

Rosen, Kenneth H., and John G. Michaels. *Handbook of Discrete and Combinatorial Mathematics.* Boca Raton, FL: CRC Press 2000.

Rositzke, Harry A. *CIA's Secret Operations: Espionage, Counterespionage, and Covert Action.* Boulder, CO: Westview Press, 1988.

Ross, David F., and J. Don Read. *Adult Eyewitness Testimony: Current Trends and Developments.* New York: Press Syndicate of the University of Cambridge, 1994.

Rossiter, Margaret. *Women in the Resistance.* New York: Praeger, 1991.

Roukis, George S., and Hugh Conway. *Global Corporate Intelligence: Opportunities, Technologies, and Threats in the 1990s.* New York: Quorum Books, 1990.

Rudgers, David F. *Creating the Secret State: The Origins of the Central Intelligence Agency,* Lawrence, KS: University of Kansas Press, 2000.

Rudman, Warren B. *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy.* Washington, D.C.: President's Foreign Intelligence Advisory Board, 1999.

Ruffner, Kevin. ed. *CORONA: America's First Satellite Program.* Washington, D.C.: CIA History Staff, 1995.

Ryan, Charles W. *Basic Electricity: A Self-Teaching Guide.* 2nd ed. New York: John Wiley & Sons, Inc., 1986.

Ryan, Ray and Lisa A. Doyle. *Basic Digital Electronics, 2nd ed.* Blue Ridge Summit, PA: Tab Books, 1990.

Sabins, F.S., Jr. *Remote Sensing Principles and Interpretation.* 2nd ed. New York: W.H. Freeman and Company, 1987.

Saferstein, Richard. *Criminalistics: An Introduction to Forensic Science.* Upper Saddle River, NJ: Prentice Hall, 1998.

Sagan, Scott D., and Kenneth N. Waltz. *The Spread of Nuclear Weapons: A Debate Renewed,* Second Edition. New York: W. W. Norton & Co., 2003.

Sage, Kingsley, and Stewart Young. "Computer Vision for Security Applications," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed. 1998.

Sakharov, Vladimir. *High Treason.* New York: Ballentine Books, 1981.

Salyers, Abigail, A., and Dixie D. Whitt. *Bacterial Pathogenesis: A Molecular Approach.* Washington, D.C.: American Society for Microbiology Press, 2001.

Sam Adams. *War of Numbers: An Intelligence Memoir.* South Royalton, Vermont: Steerforth Press, 1994.

Sayers, Michael, and Albert Eugene Kahn. *Sabotage! The Secret War against America.* New York: Harper &Brothers, 1942.

Scanlon, Charles Francis. *In Defense of the Nation: DIA at Forty Years.* Washington, D.C.: Defense Intelligence Agency, 2002.

Schecter J., and L.J. Schecter. *Sacred Secrets: How Soviet Intelligence Operations Changed American History.* Washington, D.C.: Brassey's, 2002.

Schleher, D. Curtis. *Electronic Warfare in the Information Age.* Boston: Artech House, 1999.

Schlesinger, S., S. Kinzer. *Bitter Fruit: The Untold Story of the American Coup in Guatemala.* New York: Doubleday, 1982.

Schlessinger, Monroe. *Infrared Technology Fundamentals.* New York: Marcel Dekker, 1995.

Schmidt, Gustav, ed. *A History of NATO: The First Fifty Years.* New York: Palgrave, 2001.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World.* New York: John Wiley, 2000.

Schobert, Harold H. *The Chemistry of Hydrocarbon Fuels.* Boston: Butterworth's, 1990.

Schrecker, Ellen. *Many Are the Crimes: McCarthyism in America.* Boston: Little, Brown and Company, 1998.

Schuck, P.H.H. *Agent Orange on Trial: Mass Toxic Disasters in the Courts.* Boston: Harvard University Press, 1990.

Schwartau, Winn. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption.* New York: Thunder's Mouth Press, 2000.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press, 1994.

Scientific Assessment of Ozone Depletion. vols. I and II. World Meteorological Organization Global Ozone Research and Monitoring Project, 1988.

Scientists and Engineers: Directorate for Scientific and Technical Intelligence, Directorate for Foreign Intelligence. Washington, D.C.: Defense Intelligence Agency, 1987.

Scriver, Charles R., et al. *The Metabolic and Molecular Bases of Inherited Disease,* 8th ed. New York: McGraw-Hill Professional Book Group, 2001.

Seagrave, Sterling. *Yellow Rain: A Journey Through the Terror of Chemical Warfare.* New York: M. Evans and Company, 1981.

Sebag-Montefiore, Hugh. *Enigma: The Battle for the Code.* New York: John Wiley & Sons, 2001.

Seberry, J. and J. Pieprzyk. *Cryptography: An Introduction to Computer Security.* New York: Prentice Hall, 1989.

Settles, Gary S. *Schlieren and Shadowgraph Techniques.* Heidelberg: Springer-Verlag, 2001.

Sexton, Donal J. *Signals Intelligence in World War II: A Research Guide.* Westport, CT: Greenwood Press, 1996.

Shannon, Michel L. *Bug Book: Everything You Ever Wanted To Know About Electronic Eavesdropping…But Were Afraid To Ask.* Boulder: Paladin Press, 2000.

Shaw, John M. "Jet Engines." *Magill's Survey of Science: Applied Science Series.* Edited by Frank N. McGill. Pasadena, CA: Salem Press, 1993.

Sherick, L. G. *How to Use the Freedom of Information Act (FOIA).* New York: Arco, 1978.

Sherman, Chris, and Gary Price. *The Invisible Web: Uncovering Information Sources Search Engines Can't See.* Medford, NJ: CyberAge Books, 2001.

Shevchencko, Arkady N. *Breaking with Moscow.* New York: Alfred A. Knopf, 1985.

Shnayerson, Michael, and Mark J. Plotkin. *The Killers Within: The Deadly Rise of Drug Resistant Bacteria.* New York: Little Brown & Company, 2002.

Shubert, Hiltmar, Andre Kuznetsov, and Audrey Kuznetsov. *Detection of Explosives and Landmines.* Hingham, MA: Kluwer Academic Publishers, 2002.

Shulman, Holly Cowan. *The Voice of America: Propaganda and Democracy, 1941–1945.* Madison: The University of Wisconsin Press, 1990.

Shulsky, Abram N. *Silent Warfare.* Washington, D.C.: Brassey's, 1991.

Shultz, Richard G. *The Secret War Against Hanoi: Kennedy's and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam.* New York: HarperCollins, 1999.

Sick, Gary. *All Fall Down: America's Tragic Encounter with Iran.* New York: Random House, 1985.

Sicker, Martin. *The Geopolitics of Security in the Americas: Hemispheric Denial from Monroe to Clinton.* Westport, CT: Praeger, 2002.

Siegel, J. P., and R. T. Finley. *Women in the Scientific Search* Scarecrow, 1985.

Sifakis, Carl. *Encyclopedia of Assassinations.* New York: Facts on File, 1991.

Sifton, David W., editor. *PDR Guide to Biological and Chemical Warfare Response.* Montvale, NJ: Thompson/Physician's Desk Reference, 2002.

Siljander, Raymond P. *Applied Surveillance Photography.* Springfield, IL: Thomas, 1975.

Simon, Jeffrey D. *The Terrorist Trap: America's Experience with Terrorism.* Bloomington and Indianapolis: Indiana University Press, 1994.

Sincerbox, Glenn T. *Counterfeit Deterrent Features for the Next-Generation Currency Design.* Washington, D.C.: National Academy Press, 1993.

Singer, M. and P. Berg. *Genes and Genomes.* Mill Valley, CA: University Science Books, 1991.

Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography.* New York: Doubleday, 1999.

Sittig, M. *Handbook of Toxic and Hazardous Chemicals and Carcinogens.* 3rd ed. Park Ridge, NJ: Noyes Publications, 1991.

Sivard, R. L. *World Military and Social Expenditures, 1993.* World Priorities, 1993.

Sklar, Lawrence. *Philosophy of Physics.* Boulder, CO: Westview Press, 1992.

Skolnik, Merrill I. *Introduction to RADAR Systems.* New York: McGraw Hill, 2001.

Slater, J.C. *Introduction to Chemical Physics.* New York: Dover Publications, Inc., 1939.

Slayter, Elizabeth, and Henry Slater. *Light and Electron Microscopy.* Cambridge: Cambridge University Press, 1992.

Slichter, Charles P. *Principles of Magnetic Resonance.* New York: Harper Row, 1963.

Sloane, Eugene A. *The Complete Book of Locks, Keys, Burglar and Smoke Alarms, and Other Security Devices.* New York: Morrow, 1977.

Smist, Frank John. *Congress Oversees the United States Intelligence Community, 1947–1989.* Knoxville: University of Tennessee Press, 1990.

Smith, A.D., et al. *Oxford Dictionary of Biochemistry and Molecular Biology.* New York: Oxford University Press, 1997.

Smith, Charles O. *The Science of Engineering Materials.* Englewood Cliffs, NJ: Prentice-Hall, 1969.

Smith, Dennis. *Report from Ground Zero: The Story of the Rescue Efforts at the World Trade Center.* New York: Viking, 2002.

Smith, Edward E., and R. Lednicky. *The Okhrana: The Russian Department of Police—A Bibliography.* Stanford, CA: Hoover Institution, 1967.

Smith, G. Davidson. *Combating Terrorism.* New York: Routledge, 1990.

Smith, H. C. *The Illustrated Guide to Aerodynamics.* Blue Ridge Summit, PA: Tab Books, 1992.

Smith, H., C.J. Dornan, G. Dougan, et al. (eds.). *The Activities of Bacterial Pathogens In Vivo.* River Edge, NJ: World Scientific, 2001.

Smith, Michael. *Station X: The Codebreakers of Bletchley Park.* London: Channel 4 Books, 2000.

Smith, Michael. *Station X: Decoding Nazi Secrets.* London: TV Books 2000.

Smith, Myron J., Jr. *Cloak-and-Dagger Bibliography.* Metuchen, NJ: Scarecrow Press, 1976.

Smith, R. P. *A Primer of Environmental Toxicology.* Philadelphia: Lea & Febiger, 1992.

Snider, Britt. *Sharing Secrets with Lawmakers: Congress as a User of Intelligence.* Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 1997.

Solomons, T.W. Graham. *Fundamentals of Organic Chemistry.* 5th ed. New York: John Wiley & Sons, Inc., 1997.

Sontag, Sherry. *Blind Man's Bluff: The Untold Story of American Submarine Espionage.* New York: Public Affairs, 1998.

Sorley, Lewis. *A Better War: The Unexamined Victories and Final Tragedy of America's Last Years in Vietnam.* New York: Harcourt Brace, 1999.

Sparrow, Elizabeth. *Secret Service: British Agents in France, 1792–1815.* Woodbridge, UK: Boydell Press, 1999.

Spignesi, Stephen J. *In the Crosshairs: Famous Assassinations and Attempts.* New York: New Page Books, 2003.

Spitzner, Lance. *Honeypots: Tracking Hackers.* Boston: Addison Wesley Professional, 2002.

Sproule, J. Michael. *Channels of Propaganda.* Bloomington: EDINFO Press, 1994.

Stallings, William. *Cryptography and Network Security: Principles and Practice,* 3rd. ed. Upper Saddle River, NJ: Prentice Hall, 2002.

Stanier, R.Y., J.L. Ingraham, M.L. Wheelis, and P.R. Painter. *General Microbiolgy,* 5th ed. U.K.: Macmillan Press Ltd., 1993.

Stanley, Roy M. *World War II Photo Intelligence.* New York: Scribner, 1981.

Stanley, Zell. *An Annotated Bibliography of the Open Literature on Deception.* Santa Monica, CA: RAND, 1985.

Starnes, John. *Closely Guarded: A Life in Canadian Security and Intelligence.* Toronto: University of Toronto Press, 2001.

State 2000: A New Model for Managing Foreign Affairs: Report of the U.S. Department of State Management Task Force. Washington, D.C.: U.S. Government Printing Office, 1993.

Steede-Terry, K. *Integrating GIS and the Global Positioning System.* ESRI Press, 2000.

Stephens, Frederick John, and Michael Boxall. *Fighting Knives: An Illustrated Guide to Fighting Knives and Military Survival Weapons of the World.* New York: Arco, 1980.

Stephenson, Michael, and Roger Hearn. *The Nuclear Casebook.* London: Frederick Muller Limited, 1983.

Sterling, D. *Technician's Guide to Fiber Optics (AMP).* Albany, NY: Delmar Publishers Inc., 1987.

Stern, Philip Van Doren. *Secret Missions of the Civil War.* Wings Books, New York/Avenel, NJ, 1990.

Steury, Donald P. ed. *Intentions and Capabilities: Estimates on Soviet Strategic Forces.* Washington, D.C.: History Staff, Center for the Study of Intelligence, 1996.

Steury, Donald P. ed.*On the Front Lines of the Cold War: Documents on the Intelligence War in Berlin,* Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 1999.

Stiglitz, Joseph E. *Globalization and its Discontents.* New York: W.W. Norton & Co., 2002.

Stinson, Douglas R. *Cryptography: Theory and Practice.* New York: Chapman & Hall, 2002.

Stocchi, E. *Industrial Chemistry,* vol. 1, Translated by K.A.K. Lott and E.L. Short. Chichester, West Sussex, UK: Ellis Horwood Limited, 1990.

Stokesbury, James L. *A Short History of the Korean War.* New York: W. Morrow, 1988.

Stoll, Clifford. *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York: Simon and Schuster, 2000.

Stork, David G. (ed) and Arthur C. Clarke. *HAL's Legacy: 2001's Computer Dream and Reality.* Boston: MIT Press, 1998.

Storz, Gisela, and Regine Hengge-Aronis. *Bacterial Stress Responses.* Washington: American Society for Microbiology Press, 2000.

Strachan, T. and A. Read. *Human Molecular Genetics.* New York: Bios Scientific Publishers, 1998.

Strong, Robert A. *Working in the World: Jimmy Carter and the Making of American Foreign Policy.* Baton Rouge: Louisiana State University Press, 2000.

Stutman, Robert M., and Richard Esposito. *Dead on Delivery: Inside the Drug Wars, Straight from the Street.* New York: Warner Books, 1992.

Survey of the Counterintelligence Needs of Private Industry. Washington, D.C.: National Counterintelligence Center, 1995.

Suvorov, Viktor. *Aquarium: The Career and Defection of a Soviet Spy.* London: Hamish Hamilton, 1985.

Suvorov, Viktor. *Inside Soviet Military Intelligence.* New York: Macmillan, 1984.

Syson, T. *Physics of Flying Things.* Philadelphia: Institute of Physics Publishing, 2003.

Sze, S. *The Origins of the World Health Organization: A Personal Memoir.* Boca Raton: LISZ Publications, 1982.

Szumski, Bonnie. *Latin America and U.S. Foreign Policy: Opposing Viewpoints.* St. Paul, MN: Greenhaven Press, 1988.

Tarrant, V.E. *The Red Orchestra: The Soviet Spy Network Inside Nazi Europe.* New York: John Wiley and Sons, 1995.

Taubman, Philip. *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage.* New York: Simon & Schuster, 2003.

Taylor, A. W. B. *Superfluidity and Superconductivity,* 2nd ed. Bristol: Adam Hilger, 1986.

Terrorism in the United States 1999. Washington, D.C.: Federal Bureau of Investigation, 1999.

Textbook of Medicine. 19th ed. Philadelphia: W.B. Saunders, 1994.

The EPCRA Compliance Manual: Interpreting and Implementing the Emergency Planning and Community Right-to-Know Act of 1986. Chicago: American Bar Association Section of Environment, Energy, and Resources, 1997.

Theoharis, Athan G. *A Culture of Secrecy: The Government Versus the People's Right to Know.* Lawrence: University of Kansas Press, 1998.

Thief, Geoff. "Automatic CCTV Surveillance: Towards the VIRTUAL GUARD," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed. 1999.

Thomas, D. Brian. *Viruses and the Cellular Immune Response.* New York: Marcel Dekker, 1993.

Thomas, Evan. *The Very Best Men—Four Who Dared: The Early Years of the CIA.* New York: Simon and Schuster, 1995.

Thomas, Gordon. *Gideon's Spies: The Secret History of the Mossad.* New York: St. Martin's Press, 1999.

Thompson, Kenneth W. *The President, the Bureaucracy, and World Regions in Arms Control.* Lanham, MD: University Press of America, 1998.

Thompson, Kenneth W., ed. *The Reagan Presidency.* Lanham, MD: University Press of America, 1997.

Thompson, Robert Smith. *The Missiles of October: The Declassified Story of John F. Kennedy and the Cuban Missile Crisis.* New York: Simon and Schuster, 1992.

Thompson, Scott A. *Flight Check! The Story of FAA Flight Inspection.* Washington: DOT/FAA, Office of Aviation System Standards1993.

Thompson, Stephen P. *The War on Drugs: Opposing Viewpoints.* San Diego, CA: Greenhaven Press, 1998.

Thomson, John F. *Biological Effects of Deuterium.* New York: Macmillan, 1963.

Thornborough, Anthony M. *Sky Spies: Three Decades of Airborne Reconnaissance.* London: Arms and Armour Press, 1993.

Todreas, Neil E., and Mujid S. Kazimi. *Nuclear Systems I: Thermal Hydraulic Fundamentals.* New York: Hemisphere Publishing Corporation, 1990.

Toland, John. *In Mortal Combat, Korea, 1950–1953.* New York: Morrow, 1991.

Tomedi, Rudy. *No Bugles, No Drums: An Oral History of the Korean War.* New York: Wiley, 1993.

Tonry, Michael. *Malign Neglect: Race, Crime, and Punishment in America.* Oxford University Press, 1996.

Tophoven, Rolf. *GSG 9, German Response to Terrorism.* Koblenz, Germany: Bernard & Graefe Verlag, 1984.

Tourison, Sedgwick D. *Secret Army, Secret War: Washington's Tragic Spy Operation in North Vietnam.* Annapolis, MD: Naval Institute Press, 1995.

Trask, Robert R., and Alfred Goldberg. *The Department of Defense, 1947–1997: Organization and Leaders.* Washington, D.C.: Office of the Secretary of Defense, 1997.

Trask, Roger R. *Defender of the Public Interest: The General Accounting Office, 1921–1996.* Washington, D.C.: General Accounting Office, 1996.

Trefil, James. *Encyclopedia of Science and Technology.* The Reference Works, Inc., 2001.

Troy, Thomas F. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency.* Frederick, MD: University Publications of America, 1981.

Troy, Thomas F. *Wild Bill and Intrepid, Donovan, Stephenson, and the Origin of the CIA.* New Haven: Yale University Press, 1996.

Tucker, J.B., (ed.). *Toxic Terror: Assessing the Terrorist Use of Chemical and Biological Weapons.* Cambridge: MIT Press, 2000.

Tucker, Jonathan B. *The Once and Future Threat of Smallpox.* New York: Atlantic Monthly Press, 2001.

Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition.* Boston: Houghton Mifflin, 1985.

Turvey, Brent E. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis.* San Diego, CA: Academic Press, 1999.

U.S. Central Intelligence Agency. Directorate of Intelligence. *The Russian Security Services: Sorting Out the Pieces.* Washington, D.C., 1992.

U.S. Currency: Treasury's Plan to Study Genuine and Counterfeit U.S. Currency Abroad: Report to Congressional Requesters. Washington, D.C.: General Accounting Office, 1997.

U.S. Department of State. *Foreign Relations of the United States: Department of State, 1945–1950.* Washington, D.C., 1996.

U.S. Department of Transportation Research and Development Plan. Washington, D.C.: John A. Volpe National Transportation Systems Center, 1999.

U.S. Government Printing Office. *Portals and Related Matters: Evidence Warranting Further Action by Federal Enforcement Authorities.* Washington, D.C.: U.S. Government Printing Office, 1999.

Ullman, Harlan, James P. Wade, et al. *Shock and Awe: Achieving Rapid Dominance.* Washington, D.C.: Center for Advanced Concepts and Technology, 1996.

Ullmann, John, and Steve Honeyman. *The Reporter's Handbook: An Investigator's Guide to Documents and Techniques.* New York: St. Martin's Press, 1983.

Underwood, James R., Jr. and Peter L. Guth. *Military Geology in War and Peace.* Boulder, Colorado: Geological Society of America, 1998.

United States Department of Justice and United States Department of the Treasury. *Interpol: The International Criminal Police Organization.* Washington, D.C.: Government Printing Office, 2002.

United States Department of State, Bureau of Diplomatic Security. *Countering Terrorism: Security Suggestion for U.S. Business Representatives Abroad.* Washington, D.C.: Department of State, 1999.

United States Department of State. *Foreign Relations of the United States,* Washington, D.C.: GPO, 1996.

United States General Accounting Office National Security and International Affairs Division. *Ballistic Missile Defense: Evolution and Current Issues.* Washington, D.C.: United States General Accounting Office, 1993.

United States General Accounting Office. *Chemical Safety Board: Improved Policies and Additional Oversight Are Needed.* Washington, D.C.: GPO, 2000.

United States General Services Administration. Office of Federal Protective Service. *Careers in Security and Law Enforcement.* Washington, D.C.: Government Printing Office, 2002.

United States General Services Administration. Public Buildings Service. Law Enforcement Division. *The Federal Protective Service.* Washington, D.C.: Government Printing Office, 1998.

Venkus, Robert E. *Raid on Qaddafi: The Untold Story of History's Longest Fighter Mission by the Pilot Who Directed It.* New York: St. Martin's Press, 1992.

Vinogradov, Ivan Matveevich. *Elements of Number Theory.* Dover Publications, 2003.

Vise, David A. *The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History.* New York: Atlantic Monthly Press, 2002.

Vizzard, William J. *In the Cross Fire: A Political History of the Bureau of Alcohol, Tobacco, and Firearms.* Boulder, CO: Lynne Rienner, 1997.

Volk, W., ed. *Basic Microbiology,* 7th ed. New York: Harper Collins, 1992.

Volkman, Ernest. *Espionage: The Greatest Spy Operations of the Twentieth Century.* New York: John Wiley & Sons, 1996.

Wagner, Günther, and Peter Van Den Haute. *Fission-Track Dating.* Boston: Kluwer Academic Publishers, 1992.

Wagner, Henry N., and Linda E. Ketchum. *Living with Radiation: The Risk, the Promise.* Baltimore: The Johns Hopkins University Press, 1989.

Wagnleitner, Reinhold. *Cocacolonization and the Cold War.* Chapel Hill, The University of North Carolina Press, 1997.

Walker, J. Samuel, and George T. Mazuzan. *Containing the Atom: Nuclear Regulation in a Changing Environment, 1963–1971.* Berkeley: University of California Press, 1992.

Walker, James W., and Steven Leroy De Vore. *Low Altitude Large-Scale Reconnaissance: A Method of Obtaining High Resolution Vertical Photographs for Small Areas.* Denver, CO: Interagency Archeological Services, National Park Service, 1995.

Walker, William, and Frans Berkhout. *Fissile Material Stocks: Characteristics, Measures and Policy Options.* New York: United Nations, 1999.

Wallace, John M. and Peter Hobbs. *Atmospheric Science: An Introductory Survey.* Orlando, Florida: Academic Press, Inc., 1977.

Waller, John H. *The Unseen War in Europe: Espionage and Conspiracy in the Second World War.* New York: Random House, 1996.

Walmer, Max. *An Illustrated Guide to Strategic Weapons.* New York: Prentice Hall Press, 1998.

Walpole, Ronald, and Raymond Myers, et al. *Probability and Statistics for Engineers and Scientists.* Englewood Cliffs, NJ: Prentice Hall, 2002.

Walston, Mark. *The Department of the Treasury.* New York: Chelsea House, 1989.

Walters, Peter. "CCTV Operator Performance and System Design," in proceedings from the *International Carnahan Conference on Security Technology,* Larry D. Sanson, ed. 1993.

Wang, Wallace. *Steal This Computer Book 3: What They Won't Tell You About the Internet.* San Francisco: No Starch Press, 2003.

Warner, Michael. *The Office of Strategic Services: America's First Intelligence Agency.* Washington, D.C.: CIA History Staff , Center for the Study of Intelligence, 2000.

Warner, Michael. ed. *The CIA Under Harry Truman.* Washington, D.C.: Center for the Study of Intelligence, 1994.

Warner, Roger. *Backfire: The CIA's Secret War in Laos and Its Links to the Vietnam War.* New York: Simon & Schuster, 1995.

Warren, Henry S., Jr. *Hacker's Delight.* Boston: Addison Wesley Professional, 2002.

Waterson, A. and L. Wilkinson. *An Introduction of the History of Virology.* Cambridge: Cambridge University Press, 1978.

Watson, Bruce W. *United States Intelligence: An Encyclopedia.* Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, 2000.

Watson, J.D., et al. *Molecular Biology of the Gene,* 4th ed. Menlo Park, CA: The Benjamin/Cummings Publishing Company, Inc., 1987.

Weast, Robert C. *Handbook of Chemistry and Physics.* Cleveland, OH: CRC Press, 1975.

Weber, Ralph E. ed. *Spymasters: Ten CIA Officers in Their Own Words.* Wilmington, Del: SR Books, 1999.

Weber, Ralph E. ed. *Talking with Harry: Candid Conversations with President Harry S. Truman.* Wilmington, DE: SR Books, 2001.

Webster, Daniel W. *Comprehensive Ballistic Fingerprinting of New Guns: A Tool for Solving and Preventing Violent Crime.* Baltimore, MD: Johns Hopkins Bloomberg School of Public Health, 2002.

Weintraub, Stanley. *MacArthur's War: Korea and the Undoing of an American Hero.* New York: Free Press, 2000.

Weitz, Margaret Collins. *Sisters in the Resistance : How Women Fought to Free France, 1940–1945.* New York: John Wiley & Sons., 1998.

Wells, Tim. *Four Hundred and Forty-Four Days: The Hostages Remember.* Orlando, Florida: Harcourt Brace Jovanovich Publishers, 1985.

Wentz, C. A. *Hazardous Waste Management.* New York: McGraw-Hill, 1989.

Werrell, Kenneth P. *The Evolution of the Cruise Missile.* Maxwell Air Force Base, AL: Air University Press, 1985.

Werrell, Kenneth P. *Hitting a Bullet with a Bullet: A History of Ballistic Missile Defense.* Maxwell AFB, AL: Air University Press, 2000.

West, Nigel. *The Circus: MI5 Operations 1945–1972.* New York: Stein and Day, 1983.

West, Nigel. *Molehunt: Searching for Soviet Spies in British Intelligence.* New York: Berkley, 1991.

West, Nigel. *Molehunt: Searching for Soviet Spies in MI5.* New York: W. Morrow, 1989.

West, Nigel. *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman.* New York: W. Morrow, 1988.

West, Nigel and Oleg Tsarev. *The Crown Jewels.* London: Harper Collins Publishers, 1998.

Westerby, Gerald. *In Hostile Territory: Business Secrets of a Mossad Combatant.* New York: HarperBusiness, 1998.

Westerfield, H. Bradford, ed. *Inside the CIA's Private World: Declassified Articles from the Agency's Internal Journal,* New Haven, CT: Yale University Press, 1996.

Westermeier, Reiner. *Electrophoresis in Practice.* Weinheim: Vch Verlagsgesellschaft, 2001.

Whitcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914–1917;* Chapel Hill, NC: Algonquin Books, 1989.

White, Mark. *On the Control of Silencers, Interpol: The International Criminal Police Organization.* Washington, D.C.: Government Printing Office, 2002.

White, Paul, ed. *Basic Microphones.* London: Sanctuary Press, 2000.

White, William. *The Microdot: History and Application.* Williamstown: Phillips Publications, 1992.

Whiting, Charles. *The Spymasters: The True Story of Anglo-American Intelligence Operations Within Nazi Germany, 1939–1945.* New York: Saturday Review Press, 1976.

Whitnah, Donald Robert. *U.S. Department of Transportation: A Reference History.* Westport, CT: Greenwood Press, 1998.

Whittaker, James A., and Herbert Thompson. *How to Break Software Security: Art and Science.* Boston: Addison Wesley Professional, 2002.

Williams, John B. *Image Clarity: High-Resolution Photography.* Boston: Focal Press, 1990.

Williams, Kieran, and Dennis Deletant. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania.* New York: Palgrave, 2001.

Willrich, Mason, ed. *International Safeguards and Nuclear Industry.* Baltimore, MD: Johns Hopkins Press, 1973.

Wilson, E.J.N. *An Introduction to Particle Accelerators.* Oxford: Oxford University Press, 2001.

Wilson, Jerry D. *Physics: Concepts and Applications,* 2nd edition. Lexington, MA: D. C. Heath and Company, 1981.

Wilson, William. *Dictionary of the United States Intelligence Services: Over 1500 Terms, Programs, and Agencies.* Jefferson, NC: McFarland, 1996.

Winks, Robin. *Cloak and Gown: Scholars in the Secret War,* New York: William Morrow and Company, Inc., 1987.

Winter, Gordon. *Inside BOSS: South Africa's Secret Police.* London: Allen Lane, 1981.

Winterbotham, F. W. *The Ultra Secret.* New York: Harper & Row, 1974.

Winton, John. *Ultra in the Pacific: How Breaking Japanese Codes & Cyphers Affected Naval Operations against Japan: 1941–1945.* London: Leo Cooper, 1993.

Wirtz, James J. *The Tet Offensive: Intelligence Failure in War.* Ithaca, NY: Cornell University Press, 1991.

Wise, David. *Cassidy's Run: The Secret Spy War over Nerve Gas.* New York: Random House, Inc., 2000.

Wise, David. *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America.* New York: Random House, 2002.

Witcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914–1917.* Chapel Hill, NC: Algonquin Books, 1989.

Witte, Robert S. *Statistics.* 3rd ed. New York: Holt, Rinehart and Winston, Inc., 1989.

Wittkopf, Eugene R., and James M. McCormick. *The Domestic Sources of American Foreign Policy: Insights and Evidence.* Lanham, MD: Rowman and Littefield Publishers, 1999.

Wolf, Markus. *Man Without a Face: The Autobiography of Communism's Great Spymaster.* New York: Random House, 1997.

Wolfson, Richard. *Nuclear Choices: A Citizen's Guide to Nuclear Technology.* Cambridge, Mass.: MIT Press, 1991.

Woodward, Bob. *Maestro: Greenspan's Fed and the American Boom.* New York: Simon and Schuster, 2000.

Wooldridge, E. T. *Carrier Warfare in the Pacific: An Oral History Collection.* Washington, D.C.: Smithsonian Institution Press, 1993.

Woolfson, M.M. *An Introduction to X-Ray Crystallography.* Cambridge: Cambridge University Press, 1970.

Wright, Peter. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer.* New York: Viking, 1987.

Wright, Peter. *The Spycatcher's Encyclopedia of Espionage.* Richmond and Victoria: William Heinemann Australia, 1991.

Wright, Robert K. *Military Police.* Washington, D.C.: Center of Military History, 1992.

Wyngaarden, J.B., L.H. Smith, Jr., and J.C. Bennett. *Cecil Textbook of Medicine,* 19th ed. Philadelphia: W.B. Saunders, 1992.

Wynne, Greville. *The Man from Moscow: The Story of Wynne and Penkovsky.* London: Hutchinson, 1967.

Yardley, Herbert O., *The American Black Chamber.* Indianapolis: Bobbs-Merrill,1931.

Yinon, Jehuda. *Forensic and Environmental Detection of Explosives.* New York: John Wiley & Sons, 1999.

Yoder, Andrew R., and Hank Bennett. *The Complete Shortwave Listener's Handbook.* New York: McGraw-Hill, 1997.

Young, Gray. *The Internet.* New York: H. W. Wilson, 1998.

Zacharias, Ellis M. *Secret Missions: The Story of an Intelligence Officer.* New York: G. P. Putnam's Sons, 1946.

Zegart, Amy B. *Flawed by Design: The Evolution of the CIA, JCS, and NSC.* Stanford, CA: Stanford University Press, 1999.

Zen, E-An and A. S. Walker. *Rocks and War: Geology and the Civil War Campaign of Second Manassas.* Shippensburg, Pennsylvania: White Mane Publishing, 2000.

Zim, Herbert Spencer. *Codes and Secret Writing.* New York: W. Morrow, 1948.

Zimmerman, Phillip. *The Official PGP User's Guide.* Cambridge, MA: MIT Press, 1995.

Zukin, Sharon. *Landscapes of Power: From Detroit to Disney World.* Berkeley: University of California Press, 1991.

Periodicals

Adams, Shawn. "A Beginner"s Guide to Learning Emergency Management." *Risk Management* 49, no. 5 (May 2002): 24–28.

Advisory Committee on Immunization Practices. "Recommendations of the Advisory Committee on Immunization Practices: Use of Anthrax Vaccine in the United States." *Morbidity and Mortality Weekly Report* no. 49 (2000): 1–20.

"Agency Says Engineers Likely Broke Rules." *Washington Post.* (February 29, 2000): A4.

Ahrens, Frank. "Submarines, Examined at Depth: The Smithsonian's New Nautical Exhibit Settles in for a Three-Year Tour." *Washington Post.* (May 8, 2000): C1.

Alden, Edward, and James Harding. "CIA Wins Battle to Defend U.S. Against Terror." *Financial Times.* (February 15, 2003): 1.

Alden, Edward, and Mark Turner. "Sudan's Surprise Deal with Rebels Catches Washington Off-Guard." *Financial Times.* (July 23, 2002): 10.

Alexander, Leo. "Medical Science Under Dictatorship." *New England Journal of Medicine* 241, no. 2 (1949): 39–47.

Allen, Deane J. "Reviewing the Literature: Intelligence Is Organization." *Defense Intelligence Journal* no. 1 (Spring 1992): 113–120.

Allen, Gary W., and Anthony J. Ramienski. "A Survey of Intelligence Literature." *Military Intelligence* 12, no. 2 (1986): 54–56.

Alouf, J.E. "From Diphtheritic Poison to Molecular Toxinology." *American Society for Microbiology News,* vol. 53, no. 10 (1987): 547–551.

Alper, Joseph. "Navigating Chernobyl's Deadly Maze." *Science* 5365 (May 8, 1998): 826–827.

Altmann, Jürgen. "Acoustic Weapons—A Prospective Assessment." *Science and Global Security* no. 9 (2001): 165–244.

Amar, A.R. "A Search For Justice In Our Genes." *New York Times.* 7 May 2002: A31.

Amon, Michael. "Agencies Working to Boost Security." *Washington Post.* (February 23, 2003): T1.

Anderson, Robert. "The Former Soviet Republics Are Accused of Supplying Weapons to Rogue States in Defiance of United Nation or U.S. Embargoes." *Financial Times.* (October 21, 2002): 27.

Arkin, William M. "Sci-Fi" Weapons Going to War." *Los Angeles Times.* (December 8, 2002): M1.

Arlt, R., et al. "Use of CdZnTe Detectors in Hand-Held and Portable Isotope Identifiers to Detect Illicit Trafficking of Nuclear Material and Radioactive Sources." *Nuclear Science Symposium Conference Record,* vol. 1, IEEE, 2001: 4–18–4–23.

Arney, Kevin. "Midshipman Cruises Aboard Fast Attack Submarine." *The Officer* 73, no. 11 (November 1997): 57.

Astakhova, L.N., L.R. Anspaugh, G.W. Beebe, et al. "Chernobyl-Related Thyroid Cancer in Children in Belarus." *Radiation Research* no. 150 (1998): 349–356.

Atlas, R.N. "National Security and the Biological Research Community." *Science* no. 298 (2002): 753–754.

Auer, Catherine. "EU Knocks Echelon, Wants Own Super Spy." *Bulletin of the Atomic Scientists* 57, no. 5 (September/October 2001): 11.

Auerbach, Stuart. "Party Nominees to Get Trade Briefing." *Washington Post.* (June 25, 1988): D12.

Aveni, Madonna. "Software Analyzes Potential Threats to Buildings." *Civil Engineering* 71, no. 10 (October 2001): 36.

Babbin, Jed. "Some Things Can"t Wait: Speedy Approval of New Military Technologies Will Save Lives." *Washington Times.* (June 27, 2002): A23.

Bakalar, James B. "The War on Drugs: A Peace Proposal." *The New England Journal of Medicine* (Feb 3 1994): 357–61.

Baker, Stewart A. "Don't Worry, Be Happy: Why Clipper Is Good for You." *Wired.* June 1994.

Baldauf, Scott. "Where to Find the Perfect Gift for Your 007 Wannabe." *Christian Science Monitor.* (December 7, 1999): 2.

Balding, D.J. "The DNA Database Search Controversy." *Biometrics* 58(1): 241–4 (March 2002).

Ballard, Tanya N. "Horror, then a Helping Hand." *Government Executive* 33, no. 13 (October 2001): 12–14.

Banerjee, Neela. "U.S. and Europe in Fuel Cell Pact." *New York Times.* March 7, 2003.

Barinaga, Marcia, "Asilomar Revisted: Lessons for Today?" *Science* 287 (2000).

Barnes, Scottie. "State Department Hosts Forum on Geographic Information." *Geospatial Solutions* 12, no. 9 (September 2002): 18.

Barr, Stephen. "Defense Department Agrees to Have OPM Take over Background Checks." *Washington Post.* (February 5, 2003): B2.

Barr, Stephen. "Probe's Findings Support INS Whistleblower." *Washington Post.* (December 16, 1998): A29.

Barth, Steve. "Spy vs. Spy." *World Trade* 11, no. 8 (August 1998): 34–37.

Baus, Theresa. "Dual Use Technology." *Naval Forces* 20, no. 3 (1999): S54–S55.

Baxevanis, A.D. "The Molecular Biology Database Collection: An Updated Compilation of Biological Database Resources." *Nucleic Acids Research* 29 (January 2001): 1–10.

Begley, S. "The End of Antibiotics." *Newsweek.* (28 March 1994): 47–51.

Behnisch P.A. "Biodetectors in Environmental Chemistry: Are We at a Turning Point?" *Environ Int.* 27(2001):441–2.

Belgrader, P., W. Bennet, D. Hadley, et al. "PCR Detection of Bacteria in Seven Minutes." *Science.* no. 5413: 449–450

Bennett, Charles H., and David P. DiVincenzo. "Quantum Information and Computation." *Nature* 404 (March 16, 2000): 247–255.

Bennett, Charles H., and Peter W. Shor. "Privacy in a Quantum World." *Science* no. 5415 (1999): 747–748.

Bennewitz, R., et. al. "Atomic scale memory at a silicon surface." *Nanotechnology* 13 (2000): 499–502.

Berg, P., et al. "Asilomar Conference on Recombinant DNA Molecules." *Science* no. 188 (6 June 1975): 991–994.

Bethe, Hans A., et al. "Space-Based Ballistic-Missile Defense." *Scientific American.* (October, 1984).

Betsch, D.F. "DNA Fingerprinting in Agricultural Genetics Programs." *Biotechnology Information Series (Bio-7), North Central Regional Extension Publication.* Iowa State University 1994.

Betts, K.S. "DNA Chip Technology Could Revolutionize Water Testing." *Environmental Science and Technology* no. 33 (1999): 300A–301A.

"Black September 11." *Air Force Magazine* 95, no. 9 (September 2002): 46–53.

Black, Chris. "Mitchell Urges New Classified Data Law." *Boston Globe.* (December 5, 1989): 3.

Blair, Jayson. "C.I.A. Chief Slips in to Study Police Department Program." *New York Times.* (November 6, 1999): section B, p. 2.

Bland, Timothy S. "Background Checks: Making a Federal Case." *Journal of Property Management* 64, no. 5 (September/October 2000): 26–31.

Bleek, Philipp C. "New DOE Nuclear Security Organization Begins Work." *Arms Control Today* 30, no. 3 (April 2000): 29–30.

Blumenstein, Rebecca, and Matthew Rose. "Name That Op: How U.S. Coins Phrases of War." *Wall Street Journal.* (March 24, 2003): B1.

Bodrain, Rosemarie R. "Analysis of Exempt Paint Solvents by Gas Chromatography Using Solid-Phase Microextraction." *JCT, Journal of Coatings Technology* 72, no. 900 (January 2000): 69–74.

Boguski, M.S. "The Turning Point in Genome Research." *Trends in Biochemical Sciences* 20 (August 1995): 295–296.

Bone, Margaret. "Marines Provide Safety Net to Terrorist Threat." *Leatherneck* 82, no. 2 (February 1999): 50–53.

Bonner, Raymond, et al. "Questioning Terror Suspects in a Dark and Surreal World." *New York Times.* (March 9, 2003): 1.

Bowman, M. E. "Intelligence and International Law." *International Journal of Intelligence and Counterintelligence* 8, no. 3 (fall 1995): 321–335.

Boylan, M. "Genetic Testing." *Camb Q Healthc Ethics* Summer 2002;11(3): 246–56.

Boyle, Matthew. "The Prying Game." *Fortune.* 144, no. 5 (September 17, 2001): 235.

Boyne, Sean. "Assad Purges Security Chiefs to Smooth the Way for Succession." *Jane's Intelligence Review* 11, no. 6 (June 1, 1999): 1.

Bradley, K.A., J. Mogridge, M. Mourey, et al. "Identification of the Cellular Receptor for Anthrax Toxin." *Nature* no. 414 (2001): 225–229.

Braga, Newton C. "Experimenting with Small FM Transmitters." *Poptronics* 2, no. 9 (September 2001): 41–46.

Brainard, Jeffrey. "Profiles in Pork: Wheeling Jesuit University: National Technology Transfer Center." *The Chronicle of Higher Education* 49, no. 5 (September 27, 2002): A23.

Brand, Lois. "Helping Coast Guard Enhance Port Security." *National Defense* 87, no. 590 (January 2003): 45.

Brinkley, Joel. "Coast Guard Encounters Big Hurdles in New Effort to Screen Arriving Ships." *New York Times.* (March 16, 2002): A9.

Brouwer, Greg. "Oklahoma City Complex Will Usher in New Design Criteria." *Civil Engineering* 72, no. 3 (March 2002): 16.

Brugioni, Dino A. "Satellite Images on TV: The Camera Can Lie." *Washington Post.* December 14, 1986.

Brunet, D., and D.A. Yuen. "Mantle Plumes Pinched in the Transition Zone." *Earth and Planetary Science Letters,* vol. 178 (2000): 13–27.

Bruning, Horst, and Stephen Wolff. "Automated Explosive Detection Systems Based Upon CT Technology." *Security Technology, 1998. Proceedings., 32nd Annual 1998 International Carnahan Conference.* Oct. 12–14, 1998: 55–58.

Buck, S." Searching for Graves Using Geophysical Technology: Field Tests with Ground Penetrating Radar, Magnetometry, and Electrical Resistivity." *Journal of Forensic Sciences,* vol. 48, no. 1 (2003): 5–11.

Bumiller, Elisabeth. "Government to Cover Most Costs of Insurance Losses in Terrorism." *New York Times.* (November 27, 2002): A1.

Burke, Jim. "Kids, Drugs, and Bureaucrats." *Washington Post.* (May 21, 2002): A17.

Burns, Jimmy. "Assessing Terror Threat Raises Whitehall Tension." *Financial Times.* (December 14, 2002): 5.

Burrows, W.D., and S.E. Renner. "Biological Warfare agents as Threats to Potable Water." *Environmental Health Perspectives* no. 107 (1999): 975–984.

Bush, George W. "Remarks on Signing the Terrorism Risk Insurance Act of 2002." *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2096–2097.

Bush, George W. "Statement on Signing the Intelligence Authorization Act for Fiscal Year 2002." *Weekly Compilation of Presidential Documents* 37, no. 52 (December 31, 2001): 1834.

Byrne, M.P., and L.A. Smith. "Development of Vaccines for Prevention of Botulism." *Biochimie* no. 82 (2000): 955–966.

Cabellon, Paul C. "CBIRF Takes the (Capitol) Hill." *Leatherneck* 85, no. 2 (February 2002): 19.

Caipo, M.L., S. Duffy, L. Zhao, et al." *Bacillus megaterium* Spore Germination is Influenced by Inoculum Size." *Journal of Applied Microbiology* no. 92 (2002): 879–884.

Campbell, Duncan. "U.S. Buys Up All Satellite War Images." *The Guardian (London).* October 17, 2001.

Campbell, Kurt M. "Edging Taiwan in from the Cold." *Washington Post.* (April 25, 2001): A31.

Cannon, Carl M. "Central Intelligence Agency." *National Journal* 33, no. 25 (June 23, 2001): 1903–1904.

Cao, Y.W.C., R. Jin, and C.A. Mirkin. " Nanoparticles with Raman Spectroscopic Fingerprints for DNA and RNA Detection." *Science* no. 5586 (2002): 1536–1540

Carlson, Caron. "No Threat from GSM Hackers." *Wireless Week* 5, no. 50 (December 13, 1999): 3.

Carr, Chris, Jerry Furniss, and Jack Morton. "Complying with the Economic Espionage Act." *Risk Management* 47, no. 3 (March 2000): 21–24.

Carr, Rebecca. "Security at Nuke Labs Lax—DOE "Indifferent" Despite Sept. 11." *Atlanta Journal-Constitution.* (August 20, 2002): A11.

Casagrande, R. "Technology Against Terror." *Scientific American.* 287 (2002):59–65

Caterinicchia, Dan. "When Duty Calls." *Federal Computer Week* 16, no. 36 (October 7, 2002): 25–26.

Chalmers, Bruce. "The Photovoltaic Generation of Electricity." *Scientific American.* 235, no.4 (October 1976): 34–43.

Champion, Marc. "How Do Other Countries Coordinate Security?" *Wall Street Journal.* (June 12, 2002): A14.

Chapman, Gary. "U.S.-British Cyber-Spy System Puts European Countries on Edge." *Los Angeles Times.* (August 16, 1999): 3.

Charles, Douglas M. "American, British and Canadian Intelligence Links: A Critical Annotated Bibliography." *Intelligence and National Security* 15, no. 2 (Summer 2000): 259–269.

Cho, A. "Forensic Science. Judge Reverses Decision On Fingerprint Evidence." *Science* March 2002;295(5563):2195–7.

Choffnes, E. "Germs on the Loose." *Bulletin of the Atomic Scientists* no. 57 (2001): 57–61.

Cholewka, Kathleen. "Address Management Made Easier?" *Telephony* 234, no. 1 (January 5, 1998): 39.

"Circuit Transfers Four Times More Power Out of Vibration." *Resource* 9, no. 11 (November 2002): 6.

Clellenad, C.T., V. Risca, and C. Bancroft. "Hiding Messages in DNA Microdots." *Nature* no. 399 (1999): 533–534.

Cloud, David S. and David Rogers. "Telecom Firms Lobby for Funding of Upgrades to Ease Surveillance." *Wall Street Journal.* (April 5, 2000): A4.

Cochran, William W. "Direction Finding at Ultra High Frequency (UHF): Improved Accuracy." *Wildlife Society Bulletin* 29, no. 2 (Summer 2001): 594.

Collins F.S., and V.A. McKusick. "Implications of the Human Genome Project for Medical Science." *JAMA* 285 (7 February 2001): 540–544.

Comello, Vic. "Researchers Are Giving SPME a Second Look." *Research & Development* 41, no. 2 (February 1999): 44–45.

Connolly, P. J. "Fight DDoS Attacks with Intelligence." *InfoWorld* 23, no. 39 (September 24, 2001): 58.

Costigliola, Frank. "Unceasing Penetration": Gender, Pathology, and Emotion in George Kennan's Formation of the Cold War." *Journal of American History* 83 (March, 1997): 1309–1939.

Crabb, C. "Biosensors Enliven the Science of Detection." *Chemical Engineering* August (1998): 35–39.

Crabb, Peter B. "The Use of Answering Machines and Caller ID to Regulate Home Privacy." *Environment and Behavior* 31, no. 5 (September 1999): 657–670.

Crawford, David. "Europe Eases Limits on Police, Intelligence Services—Fear of Islamist Terrorism Erodes Traditional Divide Between the Two Branches." *Wall Street Journal.* (December 17, 2002): A15.

Crawley, James W. "Details of Port Security Are Off-Limits." *San Diego Union-Tribune.* (August 23, 2002): B1.

"Crime Year in Review." *Crime Control Digest* 36, no. 35 (August 30, 2002): 1.

Croft, John. "Air Security Bill Clears Lawmakers' Logjam." *Aviation Week & Space Technology* 155, no. 21 (November 19, 2001): 46.

Csonka, E, et al. "Novel Generation of Human Satellite DNA-based Artificial Chromosomes in Mammalian Cells." *Journal of Cell Science* 113 (2000): 3207–3216.

Cummings, Jeanne, and Gary Fields. "Calculating Risks: For Two Tense Days, Bush Team Wrestled with Vague Threat." *Wall Street Journal.* (May 17, 2002): A1.

Dao, James. "Nuclear Study Raises Fears About Weapon." *New York Times.* (November 17, 2002): section 1, p. 22.

Darce, Keith. "Port Still Vulnerable, Its Chief Says." *Times-Picayune (New Orleans, LA).* (November 20, 2002): 1.

Darlington, C. D., and T.D. Lysenko (Obituary). *Nature* 266 (1977): 287–288.

DaSilva, E. "Biological Warfare, Terrorism, and the Biological Toxin Weapons Convention." *Electronic Journal of Biotechnology* 3(1999): 1–17.

Daughtry, Emily Ewell, and Fred L. Wehling. "Cooperative Efforts to Secure Fissile Material in the NIS." *Nonproliferation Review* 7, Spring 2000.

"Deadline Met for Airport Security Screeners." *San Diego Union-Tribune.* (November 17, 2002): A2.

Dean, Jason. "Taipei's Turmoil Hinders Action on Key Issues." *Wall Street Journal.* (March 21, 2002): A18.

Demmig-Adams, B., and W.W. Adams III. "Photosynthesis: Harvesting Sunlight Safely." *Nature* 403; (January 2000): 371–374.

Dempsey, D.A., H. Silva, and D.F. Klessig. "Engineering Disease and Pest Resistance in Plants." *Trends in Microbiology* no. 6 (June 1998): 54–61.

Dempsey, Judy. "EU Military Mission at Risk from Turkish Rift." *Financial Times.* (September 19, 2002): 12.

Dennis, D.T. "Tularemia." *Maxcy-Rosenau-Last Public Health and Preventive Medicine,* 14th edition. Edited by R.B. Wallace. Stamford: Appleton & Lange, 1998.

Dennis, D.T., et al. "Tularemia as a Biological Weapon." *Journal of the American Medical Association* no. 285 (June 2001): 2763–2773.

Dennis, D.T., N. Gratz, J.D. Poland, and E. Tikhomirov. *Plague Manual: Epidemiology, Distribution, Surveillance and Control.* Geneva: World Health Organization, 1999.

Denton M.D., T. Yoshida, L.L. Hsiao, R.V. Jenson, and S.R. Gullans. "DNA Microarrays: Applicability To Renal Physiology And Disease." *J. Nephrol* 2002 Mar-Apr;15 Suppl 5:S184–91.

"Designed for Danger." *Design News* 55, no. 2 (January 17, 2000): 28.

Deutch, John. "Smarter Intelligence." *Foreign Policy* no. 128 (January/February 2002): 64–69.

DeYoung, K., and Colum Lynch. "Britain Races To Rework Resolution: U.S. Insists on Limiting Concessions for Iraq." *Washington Post.* March 11, 2003.

Dezelan, Louis A. "Preparing for Terrorism." *Law & Order* 46, no. 10 (October 1998): 107–110.

Diaz-Mitoma, F., S. Paton, and A. Giulivi. "Hospital Infection Control and Bloodborne Infective Agents." *Canada Communicable Disease Report* no. 27S3 (September 2001): 40–45.

Dietrich, Bill. "Engineering—Here's What You Can Expect Next Century." *Seattle Times.* (December 15, 1992): D1.

Dire, D.J., and T.W. McGovern. "CBRNE—Biological Warfare Agents." *eMedicine Journal* 4(2002):1–39.

Dominique, Dean J. "Convoy Rat Patrol." *Army Logistician* 34, no. 3 (May/June 2002): 36–37.

Donnelly, John. "N. Korean Missile Has U.S. Range." *Boston Globe.* (February 13, 2003): A1.

Donnelly, Sally B. "Grounding the Air Marshals." *Time.* 161, no. 4 (January 27, 2003): 17.

Dooling, Dave. "Space Sentries." *IEEE Spectrum* (September, 1997): 50–59.

Duchak, G. D. "Discoverer II: A Space Architecture for Information Dominance." *Aerospace Conference Proceedings* (Vol. 7), IEEE, 1998: 9–17.

Duffy, Brian. "Terror in the Gulf: Bombs in the Desert" *U.S. News & World Report.* July 8, 1996: 28–32.

Dunlap, David W. "Architects Put on the Alert over Requests That Are Rare." *New York Times.* (October 4, 2001): B8.

Dutton, Gail. "Biotechnology Counters Bioterrorism." *Genetic Engineering News* no. 21 (December 2000): 1–22ff.

Eaglesham, Jean. "Bad Smells" Could Be Used to Disperse Crowds." *Financial Times.* (October 31, 2002): 3.

"Early Warning Technology." *Med Device Technol* 13 (2002): 70–2.

"EDM on Mission to Mars." *Manufacturing Engineering* 119, no. 4 (October 1997): 116.

Eggen, Dan, and Jim McGee. "FBI Rushes to Remake Its Mission: Counterterrorism Focus Replaces Crime Solving." *Washington Post.* (November 12, 2001): A1.

Eggen, Dan. "Bush Aims to Blend Counterterrorism Efforts." *Washington Post.* (February 15, 2003): A16.

Eggen, Dan. "FBI Seeks Data on Foreign Students; College Calls Request Illegal." *Washington Post.* (December 25, 2002): A1.

Eggen, Dan. "Hijackers Got Visas with Little Scrutiny, GAO Reports." *Washington Post.* (October 22, 2002): A7.

Elvin, John. "We've Waited Long Enough." *Washington Times.* (December 27, 1999): 26.

"E-mail and Patching Hints from NIST." *Security Management* 46, no. 7 (July 2002): 44.

Engelhard, Victor H. "How Cells Process Antigens." *Scientific American.* 271 (August 1994): 54.

Enserink, M. "Anthrax Sequence. Useful Data But No Smoking Gun." *Science* 296(5570), (May 2002): 1002–3.

"EPA Security Plan for Refining, Chemical Plants Blasted." *Oil & Gas Journal* 100, no. 39 (September 23, 2002): 22–24.

Epidemiology Program Office, CDC. "CDC's 50th Anniversary: History of CDC." *Morbidity and Mortality Weekly Report* no. 45 (1996): 525–30.

Epstein, Edward. "U.S. Has New Weapon Ready." *San Francisco Chronicle* (February 14, 2003): A1.

Ernst, Maurice. "Economic Intelligence in CIA," *Studies in Intelligence* 28, no. 4 (Winter 1984): 1–16.

Evans, D., and D. Charter. "Iraq Strikes Back with Suspected Banned Missiles." *The Times.* March 21, 2003.

Evans, J.P.O., M. Robinson, and S.X. Godber. "Pseudo-Tomographic X-Ray Imaging for Use in Aviation Security." *IEEE AES Systems Magazine,* July 1998.

Evers, Joris. "U.S. Spy Technology Failed to Signal Attack Planning." *InfoWorld* 23, no. 38 (September 17, 2001): 28.

Evers, Stacey. "DARPA to Reap Benefits of 'Energy Harvesting'." *Jane's Defence Weekly* (November 26, 1997): 8.

Fanton, Ben. "View from Above the Battlefield." *America's Civil War* 14, no. 4 (September 2001): 22–28.

Farson, S.A. "Is Canadian Intelligence Being Re-Invented?" *Canadian Foreign Policy* no. 6 (1999): 49–83.

Feder, Barnaby J. "Truth and Justice, By the Blip of a Brainwave." *New York Times.* (October 9, 2001): F3.

"FERC Streamlining to Reflect Industry." *Oil & Gas Journal* 96, no. 26 (June 29, 1998): 33.

Ferdinand, P. "Would-Be Shoe Bomber Gets Life Term." *Washington Post.* January 31, 2003; Page A1.

Ferris, John. "Coming In from the Cold War: The Historiography of American Intelligence, 1945–1990." *Diplomatic History* 19, no. 1 (Winter 1995): 87–115.

Fialka, John J. "Aftermath of Terror: Rules for Hiring Agents Are Criticized as Hampering Spy Agencies' Recruiting." *Wall Street Journal.* (September 13, 2001): A13.

"Firms Are Lining up to See." *Electronic Times* (October 16, 2000): 40.

Fisher, I. "Chief Weapons Inspectors See No Big Breakthrough After Talks in Baghdad." *New York Times.* February 10, 2003.

Flatter, J. R. "Military Police: A Force of Choice for the 21st Century MEU (SOC)." *Marine Corps Gazette* 81, no. 7 (July 1997): 36.

Foran, J.A., and T.M. Brosnan. "Early Warning Systems for Hazardous Biological Agents in Potable Water." *Environmental Health Perspectives* no. 108 (2000): 993–996.

Forden, Geoffrey, Pavel Podvig, and Theodore A. Postol. "False Alarm, Nuclear Danger." *IEEE Spectrum* (March, 2000): 31–39.

Fowler, Charles. "National Missile Defense (NMD)." *IEEE Aerospace and Electronic Systems Society (AESS) Systems Magazine* (January, 2002: 4–12.

Frank, Diane. "Cybersecurity Center Takes Shape." *Federal Computer Week* 16, no. 4 (February 18, 2002): 10.

Frank, Diane. "GSA Preps Security Pacts." *Federal Computer Week* 13, no. 6 (March 15, 1999): 1.

Frank, Diane. "NIST Aims Grants at Systems Security." *Federal Computer Week* 15, no. 11 (April 23, 2001): 12.

Frankel, Max. "Learning From the Missile Crisis." *Smithsonian* October, 2002: 53–64.

French, M. "Retinal Eyes Biometric Security. Company Reveals its Scanning Technology." *Mass High Tech. The Journal of New England Technology* 32 (2001).

Friedlander, A.M. "Tackling Anthrax." *Nature* no. 414 (2001): 160–161.

Fulghum, David A. "Microwave Weapons May Be Ready for Iraq." *Aviation Week & Space Technology* 157, no. 6 (August 5, 2002): 24.

Fund, John. "In the Fray: People Spotters—European Gizmo Tells Who's Who." *Wall Street Journal.* (January 23, 2003): D8.

Gaddis, John Lewis. "A Grand Strategy for Transformation." *Foreign Policy* no. 133 (November/December 2002): 50–57.

Garamone, Jim. "Marines to Stand up Anti-Terror Brigade." *Pentagon Brief* (October 2001): 5.

Garritsen De Vries, Margaret. "The IMF Fifty Years Later." *Finance & Development* June 1995: 43—47.

Garth, Jeff. "Retired General to Oversee Nuclear Weapons Labs." *New York Times.* (June 17, 1999): A15.

Garvey, William. "Rebirth of the Blimp." *Popular Mechanics.* 168 (1991): 30–33.

Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *Washington Post.* (June 27, 2002): A1.

Gerard, S., M. Hayes, and M. A. Rothstein. "On the Edge of Tomorrow: Fitting Genomics Into Public Health Policy." *Journal of Law, Medicine and Ethics* no. 30(3 Suppl) (2002): 173–176.

Gill, Peter. Review of *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania. Slavic Review* 61, no. 2 (2002): 375–376.

Giodano, Vincent. "Is It Right for Your Company?" *Communications News* 37, no. 9 (September 2000): 66–68.

Gips, Michael A. "Options Reviewed for Federal Building Security." *Security Management* 46, no. 7 (July 2002): 14.

Gips, Michael A. "They Secure the Body Electric." *Security Management* 46, no. 11 (November 2002): 77–81.

Girardeau, John H. "Doctrine Corner: INSCOM Intelligence Support to the Tactical Commander." *Military Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 56–57.

Gladwell, Martin. "Safety in the Skies." *New Yorker.* October 1, 2002.

Golden, Tim. "White House Wary of Cuba's Little Spy Engine That Could." *New York Times.* (January 5, 2003): p. 1, 3.

Goo, Sara Kehaulani. "Security Law Called Unconstitutional." *Washington Post.* (November 16, 2002): A12.

Goodman, Melvin A. "Science at the CIA." *Issues in Science and Technology* 18, no. 3 (Spring 2002): 90–93.

Gordievsky, Oleg. "The KGB Archives." *Intelligence and National Security* 6, no. 1 (Jan. 1991): 7–14.

Gordon, Michael R. "Radio Transmitter to Oppose Hussein Wins U.S. Support." *New York Times.* (February 28, 2002): A1.

Gordon, Michael R. "U.S. Arsenal: Treaties vs. Nontreaties." *New York Times.* (November 14, 2001): A12.

Gorman, Tom. "Rescue Worker Boot Camp." *Los Angeles Times.* (October 11, 2001): A6.

Gottlieb, Daniel W. "Keeping Trade Secrets Secret: Counterspies, Codes Courts." *Purchasing* 126 no. 7 (May 6, 1999): 24–25.

Grant, Peter. "Plots and Ploys." *Wall Street Journal.* (December 26, 2001): B4.

Greenberger, Robert S. "Dictating Terms: Sept. 11 Aids Gadhafi in Effort to Get Libya off U.S. Terrorist List." *Wall Street Journal.* (January 14, 2002): A1.

Greenfield, Ronald A. "Microbiological, Biological, and Chemical Weapons of Warfare And Terrorism." *American Journal of The Medical Sciences* 323, no. 6 (2002): 326–340.

Grier, Peter. "Hypersonic Aircraft Test Fails." *Air Force Magazine* 84, no. 8 (August 2001): 17.

Griffiths, A., et al. *Introduction to Genetic Analysis,* 7th ed. New York: W.H. Freeman and Co., 2000.

Grimm, Matthew. "A Dubious Pitch." *American Demographics* 24, no. 5 (May 2002): 44–46.

Grimsted, Patricia Kennedy. "Archives of Russia Seven Years After: 'Purveyors of Sensation or Shadows of the Past?'" *Cold War International History Project* Working Paper, no. 20, Part I. Washington, DC: CWIHP (1998).

Grimsted, Patricia Kennedy. "Russian Archives in Transition: Caught Between Political Crossfire and Economic Crisis." *The American Archivist* 56, no. 4 (Fall 1993): 618–619.

Grunwald, Michael. "Former FBI Workers File Whistleblower Suit." *Washington Post.* (October 20, 1998): A17.

Hafele, Wolf. "Energy from Nuclear Power," *Scientific American.* 263: 136–144, September, l990.

"Hainan Incident Increases Pressure in Sino-U.S. Relations." *Defense Daily International* 1, no. 2 (April 6, 2001): 14.

Hall, Mimi. "Preparations Underway for Radiation Attack." *USA Today.* (July 8, 2002): A2.

Hamer, Mick. "Airships Face a Military Future." *New Scientist* 115 (1987): 38–40.

Haque, M. Shamsul. "Government Responses to Terrorism: Critical Views of Their Impacts on People and Public Administration." *Public Administration Review* 62 (September 2002): 170–180.

Harney, R.C. "Physics and Technology of Coherent Infrared Radar." *Proceedings of the SPIE,* vol. 300 (1981).

Harris, J. "Ethical Issues in Genetic Testing for Insurance." *Law Hum Genome Rev.* 2001 Jul-Dec;(15):25–31.

Harvey, Bernard G. "Criteria for the Discovery of Chemical Elements." *Science* 193 (1976): 1271–2.

Haskell, Bob. "A Plan Well-Executed." *Soldiers* 53, no. 5 (May 1998): 38.

Haynes, V. Dion. "U.S. Works to Shore up Port Security; War Game Underscores Acute Risk." *Chicago Tribune.* (March 10, 2003): 8.

Hays, Daniel. "One-Size-Fits-All Doesn't Fit: Study." *National Underwriter* 107, no. 9 (March 3, 2003): 26.

Healy, Melissa. "Doomsday Plane's Round-the-Clock Flights Called Off." *Los Angeles Times.* (July 28, 1990): 2.

Henderson J.P. "The Use Of DNA Statistics In Criminal Trials." *Forensic Sci Int.* 2002 Aug 28;128(3):183–6.

Henderson, D.A. "Smallpox: Clinical and Epidemiologic Features." *Emerging Infectious Diseases* no. 5 (1999): 537–539.

Henderson, D.A., "The Looming Threat of Bioterrorism." *Science* no. 283 (1999): 1279–1282.

Henderson, D.A., T.V. Inglesby, J.G. Bartlett, et al. "Smallpox as a Biological Weapon: Medical and Public Health Management." *Journal of the American Medical Association* no. 281 (1999): 2127–2137.

Hentoff, Nat. "The FBI's Magic Lantern." *Village Voice.* 47, no. 22 (June 4, 2002): p. 35.

Herschensohn, Bruce. "What Proof? Terrorism Alone Is Cause for Action." *Los Angeles Times.* (October 5, 2001): B15.

Hershberg, James G. "Soviet Archives: The Opening Door." *Cold War International History Project Bulletin* 1 (Spring 1992): 1, 12.

Herskovitz, Don. "A Sampling of Direction-Finding Systems." *Journal of Electronic Defense* 23, no. 8 (August 2000): 57–65.

Hessman, James D. "The Maritime Dimension; Special Report: The Coast Guard's Role in Homeland Defense." *Sea Power* (Apr 2002), pp. 26–30.

Heywood, Karen J. "Fluid Flows in the Environment: An Introduction." *Physics Education.* 28 (1993): 43.

Hiatt, Mark. "Computers and the Revolution in Radiology." *Journal of the American Medical Association.* (April 5, 1995): 1062.

Hickey, Neil. "So Big: The Telecommunications Act at Year One." *Columbia Journalism Review* Jan/Feb. 1997: 23–28.

Higgins, Thomas V. "Technologies Merge to Create High-Density Data Storage." *Laser Focus World* (August 1993): 57–65.

Hirsch, Daniel. "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002): 38–44.

Hirsch, Michael. "Bush and the World." *Foreign Affairs* 81, no. 5 (September/October 2002): 18–44.

Hoagland, Jim. "CIA's New Old Iraq File." *Washington Post.* (October 20, 2002): B7.

Hoffman, Bruce. "Is Europe Soft on Terrorism?" *Foreign Policy* no. 115 (Summer 1999): 62–76.

Hogan, William J. "Energy from Inertial Fusion." *Physics Today* September 1992, pp. 42–50.

Hogue, Cheryl. "Regulators at Scene of Attacks." *Chemical & Engineering News* 79, no. 39 (September 24, 2001): 11.

Hollister, Anne. "Blimps." *Life Magazine.* 4 (1988): 65–69.

Holzer, T.L., J.B. Fletcher, G.S. Fuis, T. Ryberg, T.M. Brocher, and C.M. Dietel. "Seismograms Offer Insight into Oklahoma City Bombing." *Eos, Transactions American Geophysical Union,* vol. 77, no. 41 (October 8, 1996): 393, 396–397.

"Homeland Security Dept.: Is $36.2 Billion Enough?" *Aviation Week & Space Technology* 158, no. 7 (February 17, 2003): 57–58.

Horn, M.K. "Oil and Gas." *Geotimes,* vol. 40, no. 2, 1995.

Hosenball, Mark, and Greg Vistica. "The Search for Clues: Did Officials Miss Hints of an Impending Attack?" *Newsweek.* November 6, 2000:45.

House Committee on Foreign Affairs. *U.S. Policy in the Aftermath of the Bombing of Pan Am 103.* Hearing before the Subcommittees on International Security, International Organizations, and Human Rights. 103rd Cong., 2nd sess., July 28, 1994.

Houston, Betsy. "Science and Technology Is Prominent in the Department of Homeland Security." *JOM* 55, no. 1 (January 2003): 9.

"How Secure Are Your Phone, Fax, Data Transmission Systems?" *Security* 34, no. 6 (June 1997): 75–76.

Huband, Mark. "U.S. Rejected Sudanese Files on al-Qaeda." *Financial Times.* (November 30, 2001): 1.

Hughes, David. "Homeland Security Dept.: So Many Details, So Little Time." *Aviation Week & Space Technology* 157, no. 23 (December 2, 2002): 71.

Hughes, David. "New Westinghouse Airship Designed for Early Warning Surveillance." *Aviation Week & Space Technology* 135 (1991): 24–25.

Huleatt, Richard S. "Computer Supersnoop: The New Department of Homeland Security." *Information Intelligence Online Newsletter* 23, no. 12 (December 2002): 2–4.

Huleatt, Richard S. "EPIC May Never Learn Details of Government Keystroke Monitor." *Information Intelligence Online Newsletter* 22, no. 10 (October 2001): 5–6.

Hunter, David H. "The Evolution of Literature on United States Intelligence." *Armed Forces and Society* 5, no. 1 (1978): 31–52.

"IACP"s Less Lethal Force Options Course." *Law & Order* 49, no. 9 (September 2001): 95–99.

Inchniowski, Tom. "Ridge Will Face Big Challenges as Homeland Security Leader." *ENR* 250, no. 3 (January 27, 2003): 9.

Inglesby, T.V., et al. "Anthrax as a Biological Weapon." *Journal of the American Medical Association* no. 281 (May 1999): 1735–1745.

Ingram, Gregory. "Roundtable Discussion: Critical Issues in Infrastructure in Developing Countries." *Work Bank Research Observer* (1993): 473.

Ingram, Judith. "Russia Accuses U.S. of Espionage." *Chicago Sun-Times.* (April 11, 2002): 27.

International Genome Sequencing Consortium, "Initial Sequencing and Analysis of the Human Genome." *Nature* 409 (2001): 860–921.

Jackman, Tom. "Retiree Surrenders in 1975 Va. Killing." *Washington Post.* (May 22, 2002): B7.

Jackman, Tom. "Terror Suspect Allowed to Seek Foreign Aid." *Washington Post.* (July 18, 2002): B2.

Jackson, Robert L. "Sessions Concedes FBI Erred in Central American Activist Probe." *Los Angeles Times.* (February 3, 1988): 16.

Jankovic, Joseph, and Mitchell F. Brin. "The Therapeutic Uses of Botulinum Toxin." *New England Journal of Medicine* 324 (25 April 1991): 1186.

Jarvis, Ray. "Robot Navigation." *The Industrial Robot* 21, no. 2 (1994): 3.

Jayaramen, K. S. "Indian Plague Poses Enigma to Researchers." *Nature* (13 October 1994): 547.

Jeffereys, A.J. "Hypervariable 'minisatellite' Regions in Human DNA." *Nature* no. 314 (1987): 67–73.

Jeffers, B. R. "Human Biological Materials in Research: Ethical Issues and the Role of Stewardship in Minimizing Research Risks." *Advances in Nursing Science* no. 24(2) (2001): 32–46.

Jeffords, J.M., and Tom Daschle. "Political Issues in the Genome Era," *Science* 291 (16 February 2001): 1249–50.

Jeffrey, Terence P. "Two Silicon Valley Engineers Indicted for Economic Espionage Aiding China." *Human Events* 59, no. 2 (January 13, 2003): 1.

Jeffreys-Jones, Rhodri. "Review Article: Manual Indices and Digital Pathways: Developments in United States Intelligence Bibliography." *Intelligence and National Security* 9, no. 3 (Jul. 1994): 555–559.

Jeffreys-Jones, Rhodri. "The Historiography of the CIA." *Historical Journal* 23 (Jun. 1980): 489–496.

Jenkins, Sally. "Peaceful Games, Cold War Sentiment." *Washington Post.* (February 25, 2002): D1.

Jensen, Torkil H. "Fusion-A Potential Power Source." *Journal of Chemical Education,* October 1994, pp. 820–823.

Jernigan, J.A., D.S. Stevens, D.A. Ashford, et al. "Bioterrorism-Related Inhalational Anthrax: The First 10 Cases Reported in the United States." *Emerging Infectious Diseases* no. 7 (2001).

Jezek, Z. "20 Years Without Smallpox." *Epidemiology, Microbiology, and Imunology* 49, no. 3 (2000): 95–102

Johnson, George. "The Spies' Code and How It Broke." *New York Times, Week in Review.* July 16, 1995.

Johnson, Jeff. "Truckers, Shippers Blast Customs Security Plan." *Transport Topics* no. 3521 (January 27, 2003): 1.

Johnson, Jeff. "Unclear Future at Weapons Labs." *Chemical & Engineering News* 78, no. 49 (December 4, 2000): 51–58.

Johnson, K., and R. Willing. "Ex-CIA Chief Revitalizes 'truth serum' Debate." *USA Today.* (April 26, 2002): 12a.

Johnson, Kevin. "Recruits Flood Federal 'Boot Camp'." *USA Today.* (September 23, 2002): A3.

Johnston, David. "F.B.I. Warns Local Agencies to Be Aware." *New York Times.* (September 10, 2002): A17.

Johnston, David. "FBI Director Rejects Agency for Intelligence in United States." *New York Times.* (December 20, 2002): A22.

Johnston, David. "Strength Is Seen in a U.S. Export: Law Enforcement." *New York Times.* (April 17, 1995): A1.

Johnson, J. L., and Jaime R. Taylor. "Image Factorization: A New Hierarchical Decomposition Technique." *Optical Engineering,* vol. 38 (Sept 1999): 1517–23.

Johnson, J. L., M. L. Padgett, and O. Omidvar, "Overview of Pulse Coupled Neural Networks (PCNN)." *IEEE Transactions on Neural Networks,* vol. 10, Special Issue 3 (1999): 461–63.

Jones, Jerry W. "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT (Confusing, Isn't It?)" *Military Intelligence Professional Bulletin* 28, no. 2 (April-June 2002): 28–33.

Joyce, Jim. "Espionage Battleground." *Security* 40, no. 1 (January 2003): 24–25.

Kahn, A.S., S. Morse, and S. Lillibridge. "Public-Health Prepardness for Biological Terrorism in the USA." *Lancet* no. 356 (2000): 1179–1182.

Kaltenhauser, Skip. "Industrial Espionage Is Alive and Well." *World Trade* 10, no. 7 (July 1997): 24–26.

Kaplan, David E., Chitra Ragavan, Richard J. Newman, et al. "Terror's Grim Toll." *U.S. News & World Report.* October 30, 2000:32.

Karmon, Ely. "Counterterrorism Policy: Why Tehran Stops and Starts Terrorism." *Middle East Quarterly,* vol. 5, no. 4 (December 1998).

Kaufmann, A.F., M.I. Meltzer, and G.P. Schmid. "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack

Intervention Program Justifiable?" *Emerging Infectious Diseases* no. 3 (1997): 83–94.

Kedzierski, Marie. "Vaccines and Immunization (sic)." *New Scientist* 133 (8 February 1992): S1.

Kent, Cheryl. "A Safer Federal Building for Oklahoma City." *New York Times.* (August 22, 1999): 34.

Khor, Jennifer. "Information Gathering, the Law of War, and Peacekeeping." *Peacekeeping & International Relations* 24, no. 6 (November 1995): 16.

Khoury, M.J., L.L. McCabe, and E.R.B. McCabe. "Genomic Medicine: Population Screening in the Age of Genomic Medicine." *The New England Journal of Medicine* no. 348(1) (2003): 50–58.

Kilian, Michael. "Patriot Missile Miscalculations a Cause for U.S. Concern." *Chicago Tribune.* (March 27, 2003): 5.

Killian, Michael. "New Defensive Posture for Former Prosecutor: Threat from Sea a Top Priority." *Chicago Tribune.* (February 13, 2002): 7.

Kirkpatrick, Melanie. "Weapons with a Moral Dimension." *Wall Street Journal.* (January 14, 2003): A15.

Knight, Amy. "Russian Archives: Opportunities and Obstacles." *International Journal of Intelligence and Counterintelligence* 12, no. 3 (Fall 1999): 325–337.

Koper, K.D., T.C. Wallace, S.R. Taylor, and H.E. Hartse. "Forensic Seismology and the Sinking of the Kursk." *Eos, Transactions, American Geophysical Union,* vol. 82, no. 4 (2001): 37.

Koster, J.E., et al. "Alpha Detection as a Probe for Counter Proliferation." *28th Annual International Carnahan Conference on Security Technology(IEEE).* (October 1994):6–19.

Kowalski, W.J., W.P. Bahnfleth, and T.S. Whittam., "Filtration of Airborne Microorganisms: Modeling and Prediction." *ASHRAE Transactions* 105 (1999): 4–17.

Kreuzer, Heidi. "Westchester Incident Highlights Oil Spill Concerns." *Pollution Engineering* 33, no. 1 (January 2001): 9–10.

Kruse, V. J., et al. "Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems: A Probabilistic Approach." *IEEE Transactions on Power Delivery,* vol. 6, No. 3, July 1991: 1251–1263.

Ksiazek T.G., et al. "A Novel Coronavirus Associated with Severe Acute Respiratory Syndrome." *New England Journal of Medicine* 10.1056 (April 10, 2003): a030781.

Kupperschmid, David. "James Bond 'Supplier' Has the Cure for Whatever Is Bugging You." *Los Angeles Times.* (April 26, 1985): 2.

Kushner, Harvey W. "Can Security Measures Stop Terrorism?" *Security Management* 40, no. 6 (June 1996): 132.

Kuzio, Taras. "Details Emerge on Kiev's 'Alpha' Unit." *Jane's Intelligence Review* 11, no. 10 (October 1, 1999): 1.

Lacy, D.B., W. Tepp, A.C. Cohen, et al. "Crystal Structure of Botulinum Neurotoxin Type A and Implications for Toxicity." *Nature Structural Biology* no. 5 (1998): 898–902.

Ladika, Susan. "Tracing the Shadowy Origins of Nuclear Contraband." *Science* no. 5522 (2001): 1634.

Landers, Jay. "Safeguarding Water Utilities." *Civil Engineering* 72, no. 6 (June 2002): 48–53.

Lang, John. "CIA Ads Tout Career in Espionage." *Dallas Morning News.* (November 1, 1998): 15A.

Lardner, George, Jr. "Classified Trial-Data Law Attacked." *Washington Post.* (April 30, 1988): A4.

Lardner, George, Jr. "Panel Proposes Tougher Laws Against Espionage." *Washington Post.* (May 24, 1990): A16.

Lardner, Richard. "Keeping Secrets." *Government Executive* 30, no. 3 (March 1998): 27–29.

Lardner, Richard. "The Need to Know." *Government Executive* 29, no. 2 (February 1997): 16–21.

Larson, Virgil. "The Next Wave: Using Radio Frequency as Weapon." *Omaha World-Herald.* (April 14, 2002): 1D.

Lawler, Andrew. "Rules Eased on Satellite Projects." *Science* 296, no. 5566 (April 12, 2002): 237–238.

Leader, Stefan. "Cash for Carnage: Funding the Modern Terrorist." *Jane's Intelligence Review* (May 1, 1998): 36.

Leary, Warren E. "Test of Revolutionary Jet Promises to Transform Flight." *New York Times.* (May 22, 2001): F4.

LeDuc, J.W., I. Damar, J.M. Meegan, et al. "Smallpox Research Activities: U.S. Interagency Collaboration 2001." *Emerging and Infectious Diseases* 8 (2002): 743–745.

Lee, Christopher, and Sara Kehaulani Goo. "TSA Blocks Attempts to Unionize Screeners." *Washington Post.* (January 10, 2003): A19.

Lee, Christopher. "Agencies Fail Cyber Test; Report Notes 'Significant Weaknesses' in Computer Security." *Washington Post.* (November 20, 2002): A23.

Lee, Jennifer. "Guerilla Warfare, Waged with Code." *New York Times.* October 10, 2002.

Lehman, John. "Silent, Deep, Deadly." *Wall Street Journal.* (November 11, 1998): 1.

Leonard, Raymond W. "Studying the Kremlin's Secret Soldiers: A Historiographical Essay on the GRU, 1918–1945." *Journal of Military History* (Jul. 1992): 403–421.

Lester, Andrew J, and Clifton L. Smith. "Analyses of Performance of Volumetric Intrusion Detection Technologies." *Proceedings, 33rd Annual International Carnahan Conference on Security Technology.* (October 1999): 101–111–58.

"Let's Have Straight Talk on Missile Defenses." *Aviation Week & Space Technology* 145, no. 16 (October 14, 1996): 86.

Leung, W.C. "The Prosecutor's Fallacy—A Pitfall in Interpreting Probabilities in Forensic Evidence." *Med Sci Law.* 1.(2002):44–50.

Levine, Bernard. "What's Next for Electronics?" *Electronic News* 47, no. 40 (October 1, 2001): 1.

Lewis, George N., and Theodore A. Postol. "Future Challenges to Ballistic-Missile Defense." *IEEE Spectrum*, (September, 1997): 6–68.

Li Shaomin. "My Long Journey Home." *Wall Street Journal.* (August 7, 2001): A14.

Lichtblau, Eric. "FBI and CIA to Move Their Counterterror Units to a Single New Location." *New York Times.* (February 15, 2003): A14.

Lichtblau, Eric. "White House Report Stings Drug Agency on Abilities." *New York Times.* (February 5, 2003): A16.

Litke, Alan M., and Andreas S. Schwarz. "The Silicon Microstrip Detector." *Scientific American.* (May, 1995): 76.

Lombardi, Gianni. "The Contribution of Forensic Geology and Other Trace Evidence Analysis to the Investigation of the Killing of Italian Prime Minister Aldo Moro." *Journal of Forensic Sciences,* vol. 44, no. 3 (1999): 634–642.

Lombardi, Kate Stone. "Air Travel Under a More Watchful Eye." *New York Times.* (January 26, 2003): WC1.

"Looking Glass Gets a Rest at Last." *Chicago Tribune.* (July 29, 1990): 2.

Lowenthal, Mark M. "The Intelligence Library: Quantity vs. Quality." *Intelligence and National Security* 2, no. 2 (Apr. 1987): 368–373.

"Low-Power FM Transmitters." *Electronics Now* 70, no. 8 (August 1999): 37–40.

Lucia, Christine. "Counterproliferation at Core of New Security Strategy." *Arms Control Today* 32, no. 8 (October 2002): 30.

Lukasik, S. J., J. T. Goldberg, and S. E. Goodman. "Protecting an Invaluable and Ever-Widening Infrastructure." *Association for Computing Machinery* 41, no. 6 (June 1998): 11–16.

Macintrye, A,G., C.G.W. Eitzen, Jr., R. Gum, et al. "Weapons of Mass Destruction Events with Contaminated Casualties: Effective Planning for Health Care Facilities." *Journal of the American Medical Association* no. 283 (2000): 252–253.

MacLeod, Scott, Elaine Shannon, Mark Thompson, Edward Barnes, and William Dowell. "How Feuds and Culture Clashes have Stymied the USS *Cole* Investigation." *Time.* vol. 158 (July 16, 2001):38.

MacSweeney, Greg. "Caller ID with a Kick." *Insurance & Technology* 25, no. 10 (October 2000): 30–35.

Mallet, Victor. "Pretoria Faces German Bugging Protest." *Financial Times.* (November 22, 1999): 10.

Marashi, Ibrahim al-. "Iraq's Security and Intelligence Network: A Guide and Analysis." *Middle East Review of International Affairs.* 6:3 (September, 2002).

Marcus, David L. "Horror at U.S. Embassies." *Boston Globe.* (August 8, 1998): A1.

Markoff, John, and John Schwartz. "Bush Administration to Propose System for Monitoring Internet." *New York Times.* December 20, 2002.

Markoff, John. "British Concern to Help U.S. Track Terrorists." *New York Times.* (October 12, 2002): A8.

Marquand, Robert. "As War Looms, U.S. Talks to China." *Christian Science Monitor.* (October 21, 2002): 6.

Marquis, Christopher. "Some Lawmakers Urging U.S. to Speed Exports of Satellites." *New York Times.* (July 9, 2001): A7.

Marshall, Eliot. "Patriot's Scud Busting Record is Challenged." *Science* 252, no. 5006 (May 3, 1991): 640–641.

Marsili, Ray. "New Techniques Revolutionize Analyses of Liquid Samples." *Research & Development* 42, no. 2 (February 2000): 22–24.

Matthews, William. "Energy Agency Says Web Info Poses Threat." *Federal Computer Week* 16, no. 34 (September 23, 2002): 46.

Maurer, H.H. "Liquid Chromatography-Mass Spectrometry in Forensic and Clinical Toxicology." *J Chromatogr B Biomed Sci Appl.* 713 (1998): 3–25.

McCarter, Kimberly M. "Tape Recording Interviews." *Marketing Research* 8, no. 3 (fall 1996): 50–51.

McConnell, Bruce. "Telecom Role Model." *Federal Computer Week* 16, no. 40 (November 11, 2002): 27.

McCullagh, Declan. "FBI Agents Soon May Be Able to Spy on Internet Users Legally Without a Court Order." *New York Times.* (September 14, 2001.)

McManus, Doyle. "A U.S. License to Kill." *Los Angeles Times.* (January 11, 2003): A1.

McPhee, John. "Annals of Crime—The Gravel Page." *The New Yorker.* (January 29, 1996): 44–69.

Mehta, Stephanie N. "Playing Hide-and-Seek by Telephone—Phone Companies Are Arming Both Sides in the Battle to Screen Unwanted Callers." *Wall Street Journal.* (December 13, 1999): B1.

Melloan, George. "Civil Liberties Give Way to the Search for Terrorists." *Wall Street Journal.* (October 23, 2001): A27.

Melton, R. H. "Panel Criticizes U.S. Anti-Terrorism Preparedness." *Washington Post.* (December 16, 1999): A6.

Meyer, Josh. "At Least 70,000 Terrorist Suspects on Watch List." *Los Angeles Times.* (September 22, 2002): A1.

Milbank, Dana, and T. R. Reid. "New Global Threat Revives Old Alliance." *Washington Post.* (October 16, 2001): A10.

"Military Launches New EW Efforts." *Aviation Week & Space Technology* 157, no. 19 (November 4, 2002): 35–43.

"Military Operations Named." *Marine Corps Gazette* 85, no. 11 (November 2001): 4.

Miller, Bill. "National Alert System Defines Five Shades of Terrorist Threat." *Washington Post.* (March 13, 2002): A15.

Miller, Leslie. "Some Airport Screeners Raise Rates." *San Diego Union-Tribune.* (August 27, 2002): A7.

Mintz, John, and Spencer Hsu. "Customs Takes over Monitoring Local Skies." *Washington Post.* (January 28, 2003): A6.

Mintz, John. "15 Freighters Believed to Be Linked to al Qaeda." *Washington Post.* (December 31, 2002): A1.

Mintz, John. "Fearing Attack by Sea, U.S. Tracking 'Ships of Concern.'" *Seattle Times.* (December 31, 2002): A1.

Mitchell, Russ, Richard Folkers, and Susan Gregory. "Why Melissa Is So Scary." *U.S. News & World Report* (April 12, 1999): 34–36.

Molloy, Thomas. "Why Some In-Country English Language Programs Do Not Work." *DISAM: Journal of International Security Assistance Management* 24, no. 4 (summer 2002): 125–130.

Montecucco, C. (ed.). "Clostridial neurotoxins: the molecular pathogenesis of tetanus and botulism." *Current Topics in Microbiology and Immunology* no. 195 (1995): 1–278.

"Months After Anthrax Scare, Mail-Safety Goals are Unmet." *USA Today.* (August 29, 2002): 12a.

Mooney, Chris. "Spy Tech." *The American Prospect* 13, no. 2 (January 28, 2002): 39–41.

Morais, Herbert V. "The War Against Money Laundering, Terrorism, and the Financing of Terrorism." *Lawasia Journal* (2002): 1–32.

Morris, Jim. "Israel Offers Lessons in Aviation Security." *Dallas Morning News.* November 8, 2001.

"Moscow, Tehran to Discuss RF Weapons Supplies to Iran—VP." *Itar-Tass News Wire.* (February 28, 2001): 1.

Muhlebach, Richard. "What"s Your Disaster Plan?" *National Real Estate Investor* 44, no. 8 (August 2002): 64.

Mulkern, Anne C. "Agency Tackles National Security: NIST's Boulder Lab Developing Technologies to Combat Terrorism." *Denver Post.* (January 25, 2002): C1.

Mullis, K.B. and F.A. Faloona. "Specific synthesis of DNA In Vitro Via a Polymerase Catalysed Chain Reaction." *Methods in Enzymology* no. 155 (1987): 335–350.

Munro, N.B., S.S. Talmage, G.D. Griffin, et al. "The Sources, Fate, and Toxicity of Chemical Warfare Agent Degradation Products." *Environmental Health Perspectives* no. 107 (1999): 933–974.

Munro, Neil. "Fighting for Intelligence Funds." *Washington Technology* (July 27, 1995): 1.

Muradian, Vago. "Better Export Controls Needed to Check Dual-Use Technologies." *Defense Daily* 198, no. 14 (January 22, 1998): 1.

Murphy, Dean E. "As Security Cameras Sprout, Someone's Always Watching." *New York Times.* (September 29, 2002).

Myers, Steven Lee. "U.S. 'Updates' All-Out Atom War Guidelines." *New York Times.* (December 8, 1997): A3.

Nahum, Hazi, and Sheike Marom. "Aerostat-Borne Systems for Defense and Homeland Security." *Military Technology* 26, no. 8 (August 2002): 102–108.

Nakajima, T., S. Ohta, Y. Fukushima, et al. "Sequelae of Sarin Toxicity at One and Three Years After Exposure in Matsumoto, Japan." *Journal of Epidemiology* no. 9 (1999): 337–343.

Nakamura, Y., M. Leppert, P. O'Connell, et al. "Variable Number Tandem Repeat (VNTR) Markers for Human Gene Mapping." *Science* no. 237 (1987): 1616–1622.

Nasheri, Hedieh, and Timothy J. O"Hearn. "High-Tech Crimes and the American Economic Machine." *International Review of Law, Computers & Technology* 13, no. 1 (March 1999): 7–19.

National Drug Intelligence Center, United States Department of Justice. *National Drug Threat Assessment 2001: The Domestic Perspective* Johnstown, PA: National Drug Intelligence Center, October 2000.

Nelson, Scott Bernard. "U.S. Offers $5M in Financial War on Terrorism." *Boston Globe.* (November 14, 2002): C1.

"The New Department of Homeland Security." *Chemical Engineering Progress* 99, no. 2 (February 2003): 25.

"New Guidelines Offered for Emergency Response Plans." *Environmental Management Today* 7, no. 3 (July/August 1996): 5.

Newman, William W. "Reorganizing for National Security and Homeland Security." *Public Administration Review* 62 (September 2002): 126–137.

Ng Ken Boon. "Enabling Net Connection Sharing." *InternetWeek* no. 872 (August 6, 2001): 1.

"NIJ Technologies for Public Safety." *Law & Order* 50, no. 8 (August 2002).

"NIPC Loses One of Its Own to 'Beltway' Sniper." *Computerworld* 36, no. 43 (October 21, 2002): 6.

Noguchi, Yuki. "'Star Trek' Tech Gets Limited Approval." *Washington Post.* (February 15, 2002): E1.

Nolte, Carl. "Spy Store a Boon for Paranoid Public." *San Francisco Chronicle.* (January 18, 2002): A23.

Nordland, Rod; John Barry, Mark Hosenball, Debra Rosenberg, and Gregory Vistica. "A Sneak Attack: Death at Sea" *Newsweek.* October 23, 2000: 27.

"Novel Design of Countermine Robot." *Jane's International Defense Review* (February 1, 1996): 20.

Nowlan, W."A Rational View of Insurance and Genetic Discrimination." *Science* no. 297(5579) (2002): 195–196.

"Nuclear Security Gets First Director: Gordon Confirmed as GOP Blasts His Boss, Richardson." *Washington Post.* (June 15, 2000): A31.

Nye, Joseph S., Jr. "Peering into the Future." *Foreign Affairs* 73, no. 4 (July/August 1994): 82.

Oldham, Scott. "Less-Lethal Munitions." *Law & Order* 50, no. 2 (September 2002): 54–56.

Olson, James M. "The Ten Commandments of Counterintelligence." *Studies in Intelligence* no. 11 (fall-winter 2001).

Olson, Tod. "America Held Hostage: The Iranian Hostage Crisis Would Torment America and Topple a President." *Scholastic Update,* vol. 130 (May 11, 1998): 20–22.

"ONDCP Says Anti-Drug Ads Are Ineffective." *Crime Control Digest* 36, no. 20 (May 17, 2002): 4.

Opderbecke, J. "Depth Image Matching for Underwater Vehicle Navigation." *Image Processing,* vol. 2 (1999): 624–629.

O'Toole, T, "Smallpox: An Attack Scenario." *Emerging Infectious Diseases* 5 (1999): 540–546.

Ottaway, David B. "Reagan Building Vulnerable to Attack." *Washington Post.* (March 8, 1999): A1.

Pake, George E. "Nuclear Magnetic Resonance in Bulk Matter." *Physics Today* (October 1993): 46.

Palfrey, Terry. "The Hidden Legacy of Scott: Weapons of Mass Destruction and the UK Government Proposals to Control the Transfer of Technology by Intangible Means." *International Review of Law, Computers & Technology* 13, no. 2 (August 1999): 163–181.

Park, S.J, T.A. Taton, and C.A Mirkin. "Array-Based Electrical Detection of DNA with Nanoparticle Probes." *Science* no. 5559 (2002): 1503–1506.

Pasternak, D. "Wonder Weapons." *U.S. News & World Report.* July 7 (1997): 38–46.

Peake, Hayden B. "SIGINT Literature: World War I to the Present." *American Intelligence Journal* 15, no. 1 (Spring/Summer 1994): 88–92.

Perera, F.P., and I.B. Weinstein. "Molecular Epidemiology: Recent Advances and Future Directions." *Carcinogenesis* 21 (2000): 517–524.

Perry, R.D., and J.D. Fetherston. "Yersinia Pestis-Etiological Agent of Plague." *Clinical Reviews in Microbiology* no. 10 (January 1997): 35–66.

Peters, C.J., and J.W. LeDuc. "An Introduction to Ebola: The Virus and the Disease." *The Journal of Infectious Diseases* no. 179 (Supplement 1, February 1999): ix–xvi.

Peters, Katherine McIntire. "Lost in Translation." *Government Executive* 34, no. 5 (May 2002): 39–45.

Phillips, Edward H. "It Wasn't Us." *Aviation Week & Space Technology* 144, no. 15 (April 8, 1996): 19.

Phillips, Edward H. "USAF Testing CV-22 Countermeasures." *Aviation Week & Space Technology* 157, no. 15 (October 7, 2002): 59.

Piazza, Peter. "Sunset of the CIAO? Industry May Decide." *Security Management* 44, no. 11 (November 2000): 36.

Piazza, Peter. "Tools for Digital Sleuths." *Security Management* 46, no. 4 (April 2002): 36.

Pincus, Walter, and Mike Allen. "Terrorism Agency Planned: Center to Integrate Intelligence, Analysis." *Washington Post.* (January 29, 2003): A12.

Pincus, Walter. "CIA, Pentagon Back NIMA 'Concept,' Combining Spy Satellite Photo Units." *Washington Post.* (November 29, 1995): A23.

Pincus, Walter. "Computer Shutdown Hits Defense Security Service; Backlog of Background Checks Grows." *Washington Post.* (July 8, 2000): A10.

Pincus, Walter. "DOE Plan Riles Senate GOP: Choice of Richardson to Run New Bomb Agency Spurs Pay Threat." *Washington Post.* (October 19, 1999): A17.

Plotkin, Stanley A. "Vaccination in the 21st Century." *The Journal of Infectious Diseases,* vol. 168 (1993): 29–37.

Poole, Patrick. "'Echelon' Spells Trouble for Global Communications." *Privacy Journal* 25, no. 11 (September 1999): 3–4.

Porch, Douglas. "French Intelligence Culture: A Historical and Political Perspective." *Intelligence and National Security* 10, no. 3 (July 1995): 486–511.

Postel, Sandra L., and Aaron T. Wolf. "Dehydrating Conflict." *Foreign Policy* no. 126 (September/October 2001): 60–67.

Pound, Edward T. "Keeping Secrets Secret." *U.S. News & World Report.* (June 3, 2002): 22.

Pound, Edward T. "Security Panel Has Opposed Agency's Cost-Cutting Moves." *USA Today.* (August 20, 1999): 8A.

Prados, John. "Understanding Central Intelligence." *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002): 64–65.

Price, Thomas J. "Spy Stories: Espionage and the Public in the Twentieth Century." *Journal of Popular Culture* no. 30 (1996):81–89.

Priest, Dana, and Juliet Eilperin. "Panel Finds No 'Smoking Gun' in Probe of 9/11 Intelligence Failures." *Washington Post.* (July 11, 2002): A1.

Prince, Paul. "Static Electricity." *Tele.com* 6, no. 17 (September 3, 2001): 28.

Quist, D., and I.H. Chapela. "Transgenic DNA Introgressed Into Traditional Maize Landraces in Oaxaca, Mexico." *Nature* no. 414 (2001): 541–3.

Raber, E. "L-Gel Decontaminates Better Than Bleach." *Science and Technology Review,* March (2002): 10–16.

"Race to Pick a Better Cipher." *Science* no. 5382 (1998): 1411.

"RAMPART Assesses Threats." *Signal* 56, no. 1 (September 2001): 7.

Rappert, Brian. "Assessing Technologies of Political Control." *Journal of Peace Research* 36, no. 6 (November 1999): 741–750.

Reddy, Anitha. "Terrorists Are Now Targets in Money-Laundering Fight." *Washington Post.* (July 25, 2002): E3.

Reeves, A. "Tracing Biothreats with Molecular Signatures." *Los Alamos National Laboratory Research Quarterly,* Fall 2002: 15–17.

Reiss, Tom. "Now Will We Heed the Biological Threat?" *New York Times.* (February 21, 1998): 11.

"Remarks on Signing the Intelligence Authorization Act for Fiscal Year 2003." *Weekly Compilation of Presidential Documents* 38, no. 48 (December 2, 2002): 2101–2102.

"Reports Shed Light on World Trade Center Collapses, Look to Safer Structures in the Future." *JOM* 54, no. 6 (June 2002): 6.

Reppert, Barton. "Training the Tongue-Tied." *Government Executive* 34, no. 4 (April 2002): 66.

"Responses to ASR's Survey on Aviation Security Post-Sept. 11." *Airport Security Report* 9, no. 19 (September 11, 2002): 1.

Revelle, Daniel J., and Lora Lumpe. "Third World Submarines." *Scientific American.* (August 1994): 16–21.

Rhodes, Keith A. "USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis Before Implementation." *FDCH Government Account Reports* (August 22, 2002).

Rice, Condoleeza. "Anticipatory Defense in the War on Terror." *New Perspectives Quarterly* 19, no. 4 (fall 2002): 5–8.

Richardson, T. "Pitfalls in Forensic Toxicology." *Ann Clin Biochem.* 37 (2000): 20–44.

Ritchie-Matsumoto, Peggy. "Taking Your Technology to the Marketplace." *Corrections Today* 62, no. 4 (July 2000): 96–100.

Rivers, Brendan. "U.S. Navy Orders OUTBOARD Update." *Journal of Electronic Defense* 23, no. 8 (August 2000): 31.

Rivkin, David B., Jr. "The Laws of War." *Wall Street Journal.* (March 4, 2003): A14.

Robbins, J., and A.B. Schneider. "Thyroid Cancer following Exposure to Radioactive Iodine." *Reviews in Endocrine and Metabolic Disorders* no. 1 (2000): 197–203.

Robinson, C. Paul, Joan B. Woodward, and Samuel G. Varnado. "Critical Infrastructure: Interlinked and Vulnerable." *Issues in Science and Technology* 15, no. 1 (fall 1998): 61–67.

Robinson, Clarence O, Jr. "Position-Fixing Methods Use Broadband Direction Finders." *Signal* 53, no. 2 (October 1998): 71–74.

"Robo, P.I." *American Scientist* 90, no. 1 (January/February 2002): 28–29.

Romanko, J. R. "Truth Extraction." *New York Times Magazine.* (November 19, 2000): 54.

Romano, Jay. "Terrorism Insurance, at a Price." *New York Times.* (March 9, 2003): 5.

Rosenbarger, Matt. "Less-Lethal Improvements: Federal and ALS Work Together." *Law & Order* 49, no. 11 (November 2001): 84–86.

Rosenthal, E. "From China's Provinces, a Crafty Germ Spreads." *New York Times.* (April 27, 2003).

Rosenthal, S.R., M. Merchlinsky, C. Kleppinger, et al. "Developing New Smallpox Vaccines." *Emerging Infectious Diseases* no. 7 (2001): 920–926.

Rothenberg, K.H., and S.F. Terry. "Before It's Too Late—Addressing Fear of Genetic Information." *Science* no. 297(5579) (2002): 196–197.

Rubin, Debra K. "FEMA and Corps Plan New Guide for Terrorism Catastrophes." *ENR* 249, no. 15 (October 7, 2002): 14.

"Russia Developing New Radio Frequency Weapons." *Electromagnetic News Report* 30, no. 2 (March/April 2002): 1.

"S. 1447, Aviation and Transportation Security Act." *Airports* 18, no. 48 (November 27, 2001): 5.

Safire, William. "China Syndrome: Clinton's Greed for Funds Triggers a Security Meltdown." *New York Times.* (May 18, 1998): A19.

Safire, William. "Whitewash at Justice." *New York Times.* (July 16, 1999): A19.

Salamon, Julie. "A Detective-Story Approach to the Twin Towers' Collapse." *New York Times.* (April 30, 2002): E1.

Samii, Abbas William. "The Shah's Lebanon Policy: The Role of SAVAK." *Middle Eastern Studies* 33, no. 1 (January 1997): 66–91.

Sample, Ian. "Just a Normal Town." *New Scientist* 167, no. 2245 (July 1, 2000): 20.

Schaumburg, Ron. "Americans Held Hostage." *New York Times Upfront.* vol. 133(January 15, 2001): 23.

Schmemann, Serge. "Soviet Archives Provide Missing Pieces of History's Puzzles." *New York Times.* (Feb. 8, 1993).

Schmemann, Serge."Soviet Archives: Half-Open, Dirty Windows on Past." *New York Times.* (Apr. 4, 1995).

Schmidt, Susan. "DEA to Bolster Presence Along Mexican Border, in Central Asia." *Washington Post.* (August 10, 2002): A11.

Schmitt, C.K., K.C. Meysick, and A.D. O'Brien. "Bacterial Toxins: Friends or Foes?" *Emerging Infectious Diseases* no. 5 (1999): 224–234.

Schneider, Greg, and Sara Kehaulani Goo. "For Air Marshals, a Steep Takeoff." *Washington Post.* (January 2, 2003): A1.

Schneider, Greg. "No Whistleblowing Protections for Airport Baggage Screeners." *Washington Post.* (February 8, 2002): A29.

Schneider, Howard. "A Little U.S. Pop-aganda for Arabs." *Washington Post.* (July 26, 2002): A24.

Schneider, Howard. "Syria Evolves as Anti-Terror Ally." *Washington Post.* (July 25, 2002): A18.

Schoch, Deborah. "Port Security Upgrade Welcomed, But Industry Asks Who Will Pay." *Los Angeles Times.* (February 6, 2003): B3.

Schwarts, Nelson. "Learning from Israel." *Fortune.* January 21, 2002.

Schweber, Bill. "FM Transmitter/Receiver Provides 433-MHz Link." *EDN* 47, no. 9 (April 18, 2002): 22.

"Security's Growing Leftovers: Confiscated or Forgotten Objects Piling Up at Country's Airports." *Washington Post.* (February 4, 2003): E1.

Seewald, Nancy. "CIDX Forms Cybersecurity Unit." *Chemical Week* 165, no. 2 (January 15, 2003): 20.

Seffers, George I. "NIMA 'Inadequate' in Analyzing Spy Data." *Federal Computer Week* 15, no. 3 (February 5, 2001): 55.

Seife, Charles. "Crucial Cipher Flawed, Cryptographers Claim." *Science* no. 5590 (2002): 2193.

"September 11 Leaves Facility Pushed to Its Maximum." *Augusta Chronicle.* (Augusta, GA) (September 2, 2002): B5.

Serino, Robert B. "Money Laundering, Terrorism, and Fraud." *ABA Bank Compliance,* (March/April 2002): 23–26.

Settles, G.S., and W.J. McCann. "Potential for Portal Detection of Human Chemical and Biological Contamination." *SPIE Aerosense* no. 4378 (2001): paper 01.

Shams, Heba. "Using Money Laundering Control to Fight Corruption: An Extraterritorial Instrument." *International Financial and Economic Law* no. 27 (2000).

Shanker, Tom. "Largest Conventional Bomb Dropped in a Test in Florida." *New York Times.* March 12, 2003.

Sharke, Paul. "The Start of a New Movement." *Mechanical Engineering* 124, no. 8 (August 2002): 47–49.

Sipress, Alan. "Sudan Provides Administration Intelligence on Bin Laden." *Wall Street Journal.* (September 30, 2001): A14.

Skoning, Gerald. "Be Careful Not to 'Tripp.'" *HR Magazine* 43, no. 6 (May 1998): 125–130.

Skrzycki, Cindy. "Security in Mind, Customs Says Cargo Can Wait." *Washington Post.* (February 11, 2003): E1.

Slusser, Robert M. "Recent Soviet Books on the History of the Soviet Security Police—Part II." *Slavic Review* 22 (Dec. 1973): 825–828.

Smith, Bradley F. "An Idiosyncratic View of Where We Stand on the History of American Intelligence in the Early Post-1945 Era." *Intelligence and National Security* 3, no. 4 (Oct. 1988): 111–123.

Smith, Ray A. "The Aesthetics of Security—Building Owners, Architects Seek to Make Properties Safer Without Look of a Fortress." *Wall Street Journal.* (February 19, 2003): B1.

Solis, Suzanne Espinosa. "Software May Have Mapped N.Y. Hit." *San Francisco Chronicle.* (December 12, 2001): A11.

Soltis, Dan. "Integrated Emergency Response Plans Will Save U.S. Industry Millions." *Water Engineering & Management* 144, no. 2 (February 1997): 17.

Spencer, Debra D. "Vulnerability Assessment." *Corrections Today* 60, no. 4 (July 1998): 88–92.

Squeo, Anne Marie. "Leading the News: U.S. Studies Using 'E-Bomb' in Iraq—Electromagnetic Weapon Can Permanently Damage Telecom, Power Systems." *Wall Street Journal.* (February 20, 2003): A3.

Steinman, Adam H. "Streamline Your Facility's Emergency Response Plans." *Chemical Engineering* 106, no. 3 (March 1999): 102.

Stephens, Joe, and Valerie Strauss. "Retaliation Alleged at CDC; Scientist Disclosed Diversion of Funds." *Washington Post.* (August 6, 1999): A19.

Stern, Christopher. "Federal Radio Spectrum up for Bid." *Broadcasting & Cable* 124, no. 7 (February 14, 1994): 46.

Stix, Gary. "Aging Airways." *Scientific American.* (May 1994).

Stone, Richard. "Nuclear Trafficking: 'A Real and Dangerous Threat.'" *Science* no. 5522 (2001): 1632–1636.

Strong, Ronald L. "The National Drug Intelligence Center: Assessing the Drug Threat." *The Police Chief* 68, no. 5 (May 2001): 55–60.

Swanekamp, Robert. "Nuclear Renaissance Converges on Life Extension and Upgrades." *ENR* 247, no. 23 (December 3, 2001): PC54.

Sykes, L.R. "Four Decades of Progress in Seismic Identification Help Verify the CTBT." *Eos, Transactions, American Geophysical Union,* vol. 83, no. 44 (October 29, 2002): 497, 500.

Tagliabue, J. "France and Russia Ready To Use Veto Against Iraq War." *New York Times.* March 6, 2003.

Taubes, Gary. "Quantum Mechanics: To Send Data, Physicists Resort to Quantum Voodoo." *Science* 274 (Oct. 25, 1996): 504–505.

"Tech 101: Hollywood's Caller ID Hang-Up." *Los Angeles Times.* (May 24, 2001): T1.

Terpstra, David E., et al. "The Nature of Litigation Surrounding Five Screening Devices." *Public Personnel Management* 29, no. 1 (spring 2000): 43–54.

"Texas Politicians' Cases Prompt New Interest in Eavesdropping." *San Francisco Chronicle.* (December 18, 1995): A12.

"Thabo's Watching: Spying in South Africa." *The Economist* 362, no. 8266 (March 30, 2002): 41.

Thomas, Evan. "The Road to September 11." *Newsweek.* 138, no. 14 (October 1, 2001): 38–49.

Thompson, Cheryl W. "Lawmaker Faults Nuclear Facility Security Policies." *Washington Post.* (March 25, 2002): A17.

Thompson, Loren B. "The Lessons of 'Enduring Freedom.'" *Wall Street Journal.* (January 7, 2002): A24.

Thompson, Neal. "Preparing for Disaster." *The Sun.* (Baltimore, MD) (March 13, 1998): 3B.

Thompson, Phillip. "A Crystal Ball for Intelligence Needs." *Sea Power,* vol. 44, no. 3 (March 2001): 51–53.

Thormann W., Y. Aebi, M. Lanz, and J. Caslavska. "Capillary Electrophoresis in Clinical Toxicology." *Forensic Sci Int.* 92 (1998): 157–83.

Torregrosa-Penalva, German, et al. "Microwave Temperature Compensated Detector Design for Wide Dynamic Range Applications." *Microwave Journal* 44, no. 5 (May 2001): 336–346.

"Training Centers Offer Assistance." *Crime Control Digest* 36, no. 18 (May 3, 2002): 11.

Treaster, Joseph B. "Insurance for Terrorism Still a Rarity." *New York Times.* (March 8, 2003): C1.

Treherne, Jan. "Robotic Roads—Pathways to the Future." *The Industrial Robot* 21, no. 5 (1994): 3.

"TRIA Already Is a Success." *Business Insurance* 37, no. 8 (February 24, 2003): 8.

"Tuition-Free, Counter-Drug Courses Offered." *National Guard* 54, no. 10 (October 2000): 10.

Turco, R.P., A.B. Toon, T.P. Ackerman, et al. "Nuclear Winter: Global Consequences of Multiple Nuclear Explosions." *Science* no. 222 (1983): 1283–1297.

U.S. Congress. Office of Technology Assessment. *Starpower: The U.S. and the International Quest for Fusion Energy.* Washington, D.C.: Office of Technology Assessment, 1987.

U.S. Congress. Senate. Select Committee on Intelligence. *Economic Intelligence. Hearing, 103d Congress, 1st Session.* Washington, DC: GPO, 1994.

"U.S. Homeland Security: Behind the Curve in Funding and Commitment." *Aviation Week & Space Technology* 158, no. 9 (March 3, 2003): 66.

"Upgrades for P-3s to Begin in 1998." *Aviation Week & Space Technology* 146, no. 13 (March 31, 1997): 33.

"USPS Builds to Sterilize Mail." *Engineering News-Record* no. 247 (November 26, 2001): 11.

Vedantam, Shankar. "The Polygraph Test Meets Its Match." *Washington Post.* (November 12, 2001): A2.

Verton, Dan. "National IT Protection Plan Update Delayed." *Computerworld* 35, no. 41 (October 8, 2001): 12.

Verton, Dan. "NIPC Warns of Attacks, But No Impact Felt." *Computerworld* 36, no. 33 (August 12, 2002): 17.

"Victory in the War on Terrorism Will Not Be Won on the Defensive." *New York Times.* (September 10, 2002): A19.

"Virus Hits A.T.M.'s and Computers Across Globe." *New York Times.* January 28, 2003.

Vise, David A. "Senate Panel Blasts FBI's Deployment." *Washington Post.* (July 21, 2000): A29.

Vogel, Steve. "Cooler Name Prevails for 'Hot' New Marine Corps Club at Indian Head." *Washington Post.* (April 26, 2001): T15.

Wald, Matthew L. "Guards at Nuclear Plants Say They Feel Swamped by a Deluge of Overtime." *New York Times.* October 20, 2002.

Wald, Matthew L. "New Rule to Limit Boarding Passes from Gate." *New York Times.* (December 10, 2002): A24.

Wald, Matthew L. "Some Busy Airports to Miss Deadline for Scanning Bags." *New York Times.* (November 19, 2002): A23.

Waldron, Ronald J. "National Institute of Justice Helps Facilities Implement Telemedicine Program." *Corrections Today* 64, no. 2 (April 2002): 184.

Wall, Robert. "Conflict Could Test Special Ops Improvements." *Aviation Week & Space Technology* 155, no. 14 (October 1, 2001): 30–31.

Wall, Robert. "Focus on Iraq Shapes Electronic, Info Warfare." *Aviation Week & Space Technology* 157, no. 19 (November 4, 2002): 34–35.

Wall, Robert. "Intelligence Support Seen Crucial to U.N." *Aviation Week & Space Technology* 157, no. 17 (October 21, 2002): 30.

Wall, Robert. "New Arms Policies Seen Altering Warfare." *Aviation Week & Space Technology* 155, no. 10 (September 3, 2001): 100.

Wall, Robert. "Review of NMD Fallout Underway." *Aviation Week & Space Technology* 152, no. 19 (May 8, 2000): 31–32.

Wallace, T.C. "The May 1998 India and Pakistan Nuclear Tests." *Seismic Research Letters,* vol. 69 (1998): 386–393.

Waller, Douglas. "The Secret Bomb Squad." *Time.* (March 18, 2002): 23.

Wallgren, Christine. "EPA Team Does Its Work Behind the Scenes." *Boston Globe.* (August 1, 2002): 1.

Walter, K. "A Two-Pronged Attack on Bioterrorism." *Science & Technology,* June (2002): 4–11.

Wang, Wallace. "Hardening Your System." *Boardwatch* 15, no. 8 (June 2001): 44–46.

"War Spurs Aerosol Research." *Geotimes* 37 (1992): 10–11.

Warchol, Glen. "Beam Us Up, Scotty: 'Tricorder' May Fight Biological Threats." *Salt Lake Tribune.* (May 7, 2001): D1.

Warden, John A. III. "The New American Security Force." *Airpower Journal* 13, no. 3 (fall 1999): 75–91.

Warner, Tom. "U.S. Plans to Shun Ukraine President over Radar." *Financial Times.* (November 9, 2002): 10.

Watts, John M., Jr. "Our Changing World." *Fire Technology* 38, no. 2 (April 2002): 99–100.

Waugh, William L., Jr., and Richard T. Sykes. "Organizing the War on Terrorism." *Public Administration Review* 62, special issue (September 2002): 145–153.

Weckerle, J.F. "Domestic Preparedness for Events Involving Weapons of Mass Destruction." *Journal of the American Medical Association* no. 283 (1997): 435–438.

Weinberger, Caspar, and Peter Schweizer. "…But We've Defeated Terrorists Before." *USA Today.* (September 24, 2001): A15.

Weiner, Tim. "Along Borders, Tension and Uncertainty Prevail." *New York Times.* (March 1, 2003): A11.

Weiser, Carl. "'Secret' Government Site Not So Secret After All." *USA Today.* (June 26, 2002).

Wertner, C., and J. Bilbro. "Coherent Laser Radar: Technology and Applications." *Proceedings of the SPIE,* vol. 1181 (1989).

"What a Laser Can and Cannot Do." *San Jose Mercury News,* (February 1994): 22, 24.

White, Ben. "Commerce Secretary Unveils New Security Policy." *Washington Post.* (February 11, 1998): A19.

Williams, Dillwyn. "Cancer After Nuclear Fallout: Lessons From the Chernobyl Accident." *Nature Reviews,* vol. 2 (July, 2002): 543-549.

Williams, Krissah. "U.S. Seeks to Build Secure Online Network." *Washington Post.* (October 11, 2001): A10.

Williamson, Hugh. "Libya Blamed for 1986 Berlin Disco Bombing." *Financial Times.* (November 14, 2001): 12.

Wilson, George C. "Drug-War Radar Picks up a Funding Blip." *Washington Post.* (April 14, 1987): A21.

Wilson, Jim. "E-Bomb." *Popular Mechanics.* 178, no. 9 (September 2001): 50–53.

Wolkowitz, Dave. "Facility Security—Playing It Safe." *Area Development Site and Facility Planning* 37, no. 9 (September 2002): 72.

Wong, S.H. "Challenges of Toxicology for the Millennium." *Ther Drug Monit.* 22 (2000): 52–7102.

Wong, Z., V. Wilson, A.J. Jeffereys, et al. "Cloning a Selected Fragment from a Human DNA 'Fingerprint': Isolation of an Extremely Polymorphic Minisatellite." *Nucleic Acids* no. 14 (1986): 4605–46

Wright, Andrew J., et. al. "War, Recession, and Growth." *ENR* 249, no. 2 (July 8, 2002): 34–36.

Wright, Karen. "Go Ahead, Try to Lie." *Discover.* 22, no. 7 (July 2001): 21–22.

Wyman, A.R. and R. White. "A Highly Polymorphic Locus in Human DNA." *PNAS* no. 77 (1980): 6754–6758.

"Young Defends $13 Billion CVN-21 Development Investment." *Defense Daily* 217, no. 32 (February 19, 2003): 1.

Young, Emma. "Brain Scans Can Reveal Liars." *New Scientist* (November 12, 2001).

Zelikow, Philip. "The Global Infectious Disease Threat and Its Implications for the United States." *Foreign Affairs* 79, no. 4 (July/August 2000): 154–155.

ZoBell, C.E. "Bacteria as Geological Agents with Particular Reference to Petroleum." *Petroleum World* no. 10 (January 1943): 30–43.

Internet Sites

African Issues. U.S. Department of State. <http://usinfo.state.gov/regional/af/> (April 29, 2003).

Air Force Office of Special Investigations. <http://www.dtic.mil/afosi/> (December 29, 2002).

American Academy of Forensic Science. <http://www.aafs.org.> (February 7, 2003)

American Polygraph Association. <http://www.polygraph.org/> (April 15, 2003).

American Society for Microbiology. "Careers in the Microbiological Sciences." 2000. <http://www.asmusa.org/edusrc/edu21.htm> (January 22, 2002).

Arizona Department of Health Services: Epidemiology and Surveillance. "History of Biowarfare and Bioterrorism." <http://www.hs.state.az.us/phs/edc/edrp/es/bthistor2.htm>(March 12, 2003).

Army Security Agency Online. <http://www.asa.npoint.net> (December 30, 2002).

Australian Secret Intelligence Service. <http://www.asis.gov.au/> (April 1, 2003).

Australian Security Intelligence Organization. <http://www.asio.gov.au/> (April 1, 2003).

Bacteria Museum. "Special Feature: Bacterial Diseases in History." 2002. <http://www.bacteriamuseum.org/niches/features/diseasehistory.htm>l> (April 30, 2002).

Bartlett, David. *A Concise Reference Guide to the Metric System.* <http://www.bms.abdn.ac.uk/undergraduate/guidetounits.html> (2002).

Biosensor Technologies. <http://www.darpa.mil/dso/thrust/biosci/biosensor/index.html> (March 11, 2003).

Brookhaven National Laboratory. <http://www.bnl.gov/world/> (April 2, 2003).

Brookings Institution. <http://www.brookings.edu> (February 27, 2003).

Bureau for International Narcotics and Law Enforcement Affairs. <http://www.state.gov/g/inl/> (March 19, 2003).

Bureau of Alcohol, Tobacco, and Firearms. <http://www.atf.treas.gov> (December 30, 2002).

Bureau of Citizenship and Immigration Services. INSPASS. March 1, 2003. <http://www.immigration.gov/graphics/howdoi/inspassloc.htm> (April 14, 2003).

Bureau of Engraving and Printing. <http://www.bep.treas.gov/> (February 5, 2003).

Bureau of Intelligence and Research. U.S. Department of State. <http://www.state.gov/s/inr/> (April 7, 2003).

Careers in Intelligence. Association of Former Intelligence Officers. <http://www.afio.com/sections/careers/> (April 30, 2003).

CDC. "Severe Acute Respiratory Syndrome (SARS)." April 3, 2003. <http;//www.cdc.gov/ncidod/sars/isolationquarantine.htm> (April 27, 2003).

CDI (Center for Defense Information), Terrorism Project. CDI Fact Sheet: Current List of Designated Foreign Terrorist Organizations. March 27, 2003. <http://www.cdi.org/terrorism/terrorist.cfm> (April 17, 2003).

Center for Strategic and International Studies. <http://www.csis.org> (February 27, 2003).

Centers for Disease Control. "Anthrax." 2001. <http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_t.htm> (January 27, 2002).

Centers for Disease Control. "Biological Diseases/Agents Listing." 2001. <http://www.bt.cdc.gov/Agent/Agentlist.asp> (January 23, 2002).

Centers for Disease Control. "Ebola Hemorrhagic Fever." 2001. <http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.htm> (March 12, 2003).

Centers for Disease Control. "Viral Hemorrhagic Fevers." 2000. <http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/vhf.htm> (March 12, 2003).

Centers for Disease Control. "Yellow Fever: Disease and Vaccine." 2001. <http://www.cdc.gov/ncidod/dvbid/yellowfever/index.htm> (March 12, 2003).

Centers for Disease Control and Prevention. "About CDC." November 2, 2002. <http://www.cdc.gov/aboutcdc.htm> (December 28, 2002).

Centers for Disease Control and Prevention: "Facts About Sarin." <http://www.bt.cdc.gov/agent/sarin/basics/facts.asp> (March 25, 2003).

Central Intelligence Agency. <http://www.cia.gov/> (April 24, 2003).

Central Intelligence Agency. "Center for Studies of Intelligence." <http://www.cia.gov/csi/> (January 17, 2003).

Central Intelligence Agency. Federation of American Scientists. <http://www.fas.org/irp/cia/index.html> (April 24, 2003).

Central Intelligence Agency. "The Global Infectious Disease Threat and Its Implications for the United States." January 2000.<http://www.cia.gov/cia/publications/nie/report/nie99–17d.html> (November 22, 2002).

Central Intelligence Agency. "Key Events in CIA's History." <http://www.cia.gov/cia/publications/facttell/keyevent.htm> (January 2, 2003).

Central Intelligence Agency. *The Office of Strategic Services: America's First Intelligence Agency.* <http://www.cia.gov/cia/publications/oss/> (March 1, 2003)

Central Intelligence Agency. World Factbook, 2002. <http://www.cia.gov/cia/publications/factbook/> (April 16, 2003).

Chemical and Biological Information Analysis Center. <http://www.cbiac.apgea.army.mil/> (January 17, 2003).

"The CERN Archive." <http://library.cern.ch/archives/index.html> (March 11, 2003).

CIA Careers. Central Intelligence Agency. <http://www.cia.gov/employment/> (April 30, 2003).

CIA Museum. Central Intelligence Agency. <http://www.cia.gov/cia/information/artifacts/> (March 29, 2003).

Coast Guard National Response Center. <http://www.nrc.uscg.mil/index.htm> (January 22, 2003).

Communications Electronics Security Group. <http://www.cesg.gov.uk/> (April 12, 2003).

"The Comprehensive Nuclear Test-Ban Treaty." United States Department of State. <http://www.state.gov/www/global/arms/treaties/ctb.html> (March 10, 2003).

Computer Security Division. National Institute of Standards and Technology. <http://csrc.nist.gov> (January 28, 2003).

Coordinator for Counterterrorism. United States Department of State. <http://www.state.gov/s/ct/> (February 22, 2003).

Council on Foreign Relations. "Loose Nukes." 2003. <http://www.terrorismanswers.com/weapons/loosenukes_print.html> (February 28, 2003).

Counterfeit Detection: A Guide to Spotting Counterfeit Currency. <http://www.indigoimage.com/> (February 5, 2003).

Counterterrorism and Incident Response. Lawrence Livermore National Laboratory. <http://www.llnl.gov/nai/rdiv/rdiv.html> (April 2, 2003).

Counterterrorism Policy. University of Pittsburgh School of Law. <http://jurist.law.pitt.edu/terrorism/terrorism2.htm> (May 1, 2003).

Court Technology Laboratory. "Biometrics and the Courts. Individual biometrics." <http://ctl.ncsc.dni.us/>(December 14, 2002).

Critical Infrastructure Assurance Office. <http://www.ciao.gov> (January 28, 2003).

Declassification and Freedom of Information Act (FOIA). Defense Prisoner of War/Missing Personnel Office. <http://www.dtic.mil/dpmo/foia/> (January 21, 2003).

Declassified Intelligence Satellite Photographs. <http://mac.usgs.gov/isb/pubs/factsheets/fs09096.html> (February 13, 2003).

Defense Advanced Research Projects Agency. <http://www.darpa.mil/> (April 14, 2003).

Defense Advanced Research Projects Agency, Defense Science Office. Continuous Assisted Performance (CAP). <http://www.darpa.mil/dso/thrust/biosci/cap.htm> (April 14, 2003).

Defense Department Space Policy. Federation of American Scientists. <http://www.fas.org/spp/military/docops/defense/d5105_19.htm> (February 22, 2003).

Defense Information Systems Agency. <http://www.disa.mil/> (February 22, 2003).

Defense Intelligence Agency. <http://www.dia.mil/> (April 14, 2003).

Defense Intelligence Agency. Federation of American Scientists. <http://www.fas.org/irp/dia/> (April 14, 2003).

Defense Language Institute Foreign Language Center. <http://pom-www.army.mil/> (April 4, 2003).

Defense Nuclear Facilities Safety Board. <http://www.dnfsb.gov> (February 22, 2003).

Defense Security Service. <http://www.dss.mil/> (February 22, 2003).

Department of Energy. <http://www.energy.gov> (March 7, 2003).

Department of Energy Office of Security. <http://www.so.doe.gov> (March 7, 2003).

Department of Homeland Security. April 2, 2003. <http://www.dhs.gov/dhspublic/index.jsp> (April 11, 2003).

Department of Homeland Security, Bureau of Citizenship and Immigration Services. Law Enforcement: The National Border Patrol Strategy. <http://www.immigration.gov/graphics/publicaffairs/statements/igstate.htm> (April 12, 2003).

Department of Homeland Security Reorganization. C-SPAN. <http://www.c-span.org/homelandsecurity/chart.asp> (April 11, 2003).

Department of State. U.S. Intelligence Community. <http://www.intelligence.gov/1-members_state.shtml> (April 7, 2003).

Digital Globe. <http://www.digitalglobe.com/>(April 12, 2003).

Directorate of Science and Technology. Central Intelligence Agency. <http://www.cia.gov/cia/dst/home.html> (April 24, 2003).

Drug Enforcement Administration. <http://www.dea.gov> (March 13, 2003).

Dual Use Science and Technology Program. <http://www.dtic.mil/dust/> (April 14, 2003).

Earthshots: Satellite Images of Environmental Change (U.S. Geological Survey). <http://edcwww.cr.usgs.gov/earthshots/slow/tableofcontents> (February 26, 2003).

"Electromagnetic Spectrum Use in Joint Military Operations." Chairman of the Joint Chiefs of Staff Instruction. May 1, 2000. <http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3320_01.pdf> (January 30, 2003).

Emergency Response Program, National Response Team. Environmental Protection Agency. <http://www.epa.gov/superfund/programs/er/nrs/nrsnrt.htm> (March 30, 2003).

Environmental Measurements Laboratory. National Security. <http://www.eml.doe.gov/> (March 16, 2003).

Environmental Protection Agency, Office of Water 2002. <http://www.epa.gov/owow/estuaries/about1.htm> (May, 11, 2002).

EPA's Radiation Protection Program: Emergency Response. Environmental Protection Agency. <http://www.epa.gov/radiation/rert/history.htm> (March 4, 2003).

Evaluation Report on Measurement and Signature Intelligence. <http://www.fas.org/irp/program/masint_evaluation_rep.htm> (January 17, 2003).

Executive Orders. National Archives and Records Administration. <http://www.archives.gov/federal_register/executive_orders/executive_orders.html>(January 22, 2003).

FBI Laboratory Explosives Unit. <http://www.fbi.gov/hq/lab/org/eu.htm> (January 16, 2003).

Federal Bureau of Investigation. <http://www.fbi.gov> (May 4, 2003).

Federal Emergency Management Agency. <http://www.fema.gov> (March 26, 2003).

Federal Energy Regulatory Commission. <http://www.ferc.fed.us/> (February 23, 2003).

Federal Law Enforcement Training Center. <http://www.fletc.gov> (March 19, 2003).

Federal Radiological Emergency Response Plan. Florida Department of Community Affairs. <http://www.dca.state.fl.us/bpr/EMTOOLS/Nuclear/frerp.htm> (March 4, 2003).

Federal Reserve Board. <http://www.federalreserve.gov/> (February 5, 2003).

Federation of American Scientists. "Central Intelligence Agency." September 23, 1996. <http://www.fas.org/irp/cia/ciahist.htm> (January 2, 2003).

Federation of American Scientists, FAS Intelligence Resource Program. "Soviet/Russian Intelligence Agencies." <http://www.fas.org/irp/world/russia/> (April 18, 2003).

Foreign Emergency Support Team. U.S. Department of State. <http://www.state.gov/s/ct/rls/fs/2002/13045.htm> (February 23, 2003).

Foreign Service Institute. <http://www.state.gov/m/fsi/> (April 4, 2003).

Forensic Science Center , University of California Lawrence Livermore National Laboratory. <http://www.llnl.gov/IPandC/op96/10/10h-for.html.> (7 February 2003)

Freedom of Information Act (FOIA). U.S. Department of Justice. <http://www.usdoj.gov/04foia/> (March 16, 2003).

GAO Report: Patriot Missile Defense. Federation of American Scientists. <http://www.fas.org/spp/starwars/gao/im92026.htm> (April 7, 2003).

General Accounting Office. <http://www.gao.gov/> (February 23, 2003).

General Services Administration. <http://www.gsa.gov/> (February 23, 2003).

Global Analytic Information Technology Services. "Retinal Scanning." <http://www.gaits.com/biometrics_retinal.asp> (December 14, 2002).

Government Communications Headquarters. <http://www.gchq.gov.uk/> (April 12, 2003).

"Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection (NIJ Guide 602–00)." Institute of Justice, U.S. Department of Justice. February, 2001. <http://www.ojp.usdoj.gov/nij/pubs-sum/184432.htm> (April 23, 2003).

Haze Gray and Underway World Aircraft Carrier Lists. <http://www.hazegray.org/navhist/carriers/> (April 13, 2003).

Heritage Foundation. <http://www.heritage.org> (February 27, 2003).

History of the National Security Council. American Federation of Scientists. <http://www.fas.org/irp/offdocs/NSChistory.htm> (March 24, 2003).

Hoover Institution. <http://www-hoover.stanford.edu> (February 27, 2003).

Human Genome Project. "From the Genome to the Proteome." <http://www.ornl.gov/TechResources/Human_Genome/project/info.html> (March 14, 2003).

ID Theft Resource Center. "ID Theft." October 28, 2002. <http://www.idtheftcenter.org/> (December 1, 2002).

Imagery Intelligence. Federation of American Scientists. <http://www.fas.org/irp/imint/> (April 3, 2003).

ImageSat International. <http://www.imagesatintl.com/>(12 April 2003).

Information Warfare and Information Security on the Web. Federation of American Scientists. <http://www.fas.org/irp/wwwinfo.html> (April 14, 2003).

The Information Warfare Site. <http://www.iwar.org.uk/> (April 14, 2003).

Institute for Genomic Research. "About TIGR." 2002. <http://www.tigr.org/about/> (May 3, 2002).

Institute for the Advanced Study of Information Warfare. <http://www.psycom.net/iwar.1.html> (April 14, 2003).

Intelligence Agency Profiles. Federation of American Scientists. <http://www.fas.org/irp/agency/> (April 14, 2003).

Internal Revenue Service. <http://www.irs.gov/> (April 4, 2003).

International Atomic Energy Agency (IAEA). 2003. <http://www.iaea.org/worldatom/> (April 2, 2003).

International Committee of the Red Cross. "Depleted Uranium Munitions." June 6, 2001. <http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/57JR5D?OpenDocument> (March 6, 2003).

International Spy Museum. <http://www.spymuseum.org> (January 31, 2003).

The Internet Dermatology Society. "Biological Warfare and its Cutaneous Manifestations." <http://telemedicine.org/BioWar/biologic.htm> (May 10, 2002).

Jane's. <http://www.janes.com> (February 27, 2003).

Jasinski, Michael. "Nonproliferation Assistance to Russia and the New Independent States." Center for Nonproliferation Studies for the Nuclear Threat Initiative. August 2002. <http://www.nti.org/e_research/e3_4b.html> (February 28, 2003).

Lawrence Livermore National Laboratories. "Chemical and Biological Detection Technologies." <http://www.llnl.gov/nai/rdiv/chbio.html> (January 15, 2003).

"The Limited Nuclear Test-Ban Treaty." United States Department of State. <http://www.state.gov/t/ac/trt/4797.htm> (March 10, 2003).

Los Alamos National Laboratory. <http://www.lanl.gov/worldview/> (March 23, 2003).

MI5: The Security Service. <http://www.mi5.gov.uk/> (April 11, 2003).

National Atmospheric Release Advisory Center. <http://narac.llnl.gov/> (January 14, 2003).

National Center for Forensic Science, University of Central Florida. <http://ncfs.ucf.edu/navbar.html.> (February 7, 2003)

National Communication System. <http://www.ncs.gov> (January 29, 2003).

National Domestic Preparedness Office. Federation of American Scientists. <http://www.fas.org/irp/agency/doj/fbi/ndpo/> (March 28, 2003).

National Drug Intelligence Center. <http://www.usdoj.gov/ndic/> (February 23, 2003).

National Foreign Language Center. University of Maryland. <http://www.nflc.org/> (April 4, 2003).

National Human Genome Research Institute. "Ethical, Legal and Social Implications of Human Genetic Research." (October 2000). <http://www.nhgri.nih.gov/ELSI/> (June 15, 2002).

National Imagery and Mapping Agency. "Shuttle Radar Topography Mission Navigation Page." October 11, 2002. <http://www.nima.mil/srtm/navigation.html> (December 9, 2002).

National Infrastructure Protection Center. <http://www.nipc.gov> (March 4, 2003).

National Institute of Justice. <http://www.ojp.usdoj.gov/nij/> (March 28, 2003).

National Institute of Mental Health <http://www.nimh.nih.gov/> (December 7, 2002).

National Institute of Standards and Technology. <http://www.nist.gov/> (January 28, 2003).

National Institutes of Health. <http://www.nih.gov.> (January 1, 2003).

National Intelligence Council. <http://www.cia.gov/nic/> (March 17, 2003).

National Interagency Civil-Military Institute. <http://www.nici.org/> (March 30, 2003).

National Maritime Intelligence Center/Office of Naval Intelligence. <http://www.nmic.navy.mil/nmicpic.htm> (January 17, 2003).

National Nuclear Security Administration. <http://www.nnsa.doe.gov> (March 7, 2003).

National Oceanic & Atmospheric Administration (NOAA). <http://www.noaa.gov> (May 10, 2003).

National Reconnaissance Office. <http://www.nro.gov/> (April 1, 2003).

National Science Foundation. <http://www.nsf.gov> (January 15, 2003).

National Security Agency. <http://www.nsa.gov/> (March 24, 2003).

National Security Agency. Federation of American Scientists. <http://www.fas.org/irp/nsa/index.html> (March 24, 2003).

National Security Council. <http://www.whitehouse.gov/nsc/> (March 24, 2003).

National Security Strategy of the United States of America. <http://www.whitehouse.gov/nsc/nss.html> (March 18, 2003).

National Security Telecommunications Advisory Committee. <http://www.ncs.gov/NSTAC/nstac.htm> (February 2, 2003).

National Technology Transfer Center. <http://www.nttc.edu> (March 18, 2003).

National Telecommunications and Information Administration. <http://www.ntia.doc.gov/> (March 28, 2003).

National Weather Service. <http://www.nws.noaa.gov> (April 30, 2003).

NATO. "North Atlantic Treaty Organisation." January 31, 2003. <http://www.nato.int/> (February 1, 2003).

Naval Criminal Investigative Service. <http://www.ncis.navy.mil> (January 18, 2003).

Naval Special Warfare. <http://www.sealchallenge.navy.mil> (April 1, 2003).

NSA Career Center. National Security Agency. <http://www.nsa.gov/programs/employ/homepage.html> (April 30, 2003).

"Nuclear Security—Before and After September 11." U.S. Nuclear Regulatory Commission. September 23, 2002. <http://www.nrc.gov/what-we-do/safeguards/response-911.html> (December 11, 2002).

Office of Domestic Preparedness. U.S. Department of Justice. <http://www.ojp.usdoj.gov/odp/> (March 28, 2003).

Office of Information Security. General Service Administration Federal Technology Service. <http://www.fts.gsa.gov/infosec/> (March 4, 2003).

Office of Intelligence Policy and Review. Department of Justice. <http://www.usdoj.gov/oipr/> (March 15, 2003).

Office of Intelligence Support. Federation of American Scientists. <http://www.fa.org/irp/agency/ustreas/tdois.htm> (March 17, 2003).

Office of the National Counterintelligence Executive. <http://www.ncix.gov> (March 17, 2003).

Office of the Public Health Service Historian. <http://lhncbc.nlm.nih.gov/apdb/phsHistory.> (October 19, 2000).

Office of the Surgeon General. <http://www.surgeongeneral.gov/> (April 2, 2003).

Official Intelligence Documents. American Federation of Scientists. <http://fas.org/irp/offdocs/> (March 24, 2003).

Online Career Center. Intelligence Careers. <http://www.intelligencecareers.com/_homeroom/index.cfm> (April 30, 2003).

Pharmaceutical Researchers and Manufacturers of America "Genomics: A Global Resource"<http://genomics.phrma.org/> (April 3, 2003).

Physicians and Scientists for Responsible Application of Science and Technology. "How Are Genes Engineered?" 2001. <http//www.psrast.org/whisge.htm> (June 15, 2002).

Plum Island Animal Disease Center. <http://www.ars.usda.gov/plum/index.html> (March 23, 2003).

Port Security Units. U.S. Coast Guard. <http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PSUs.html> (March 29, 2003).

Poxvirus Bioinformatics Resource Center <http://www.poxvirus.org/> (April 1, 2003).

Pravda. <http://english.pravda.ru/> (April 30, 2003).

Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counterterrorism. Federation of American Scientists. <http://www.fas.org/irp/news/1998/05/980522-wh3.htm> (March 26, 2003).

RAND. <http://www.rand.org> (February 27, 2003).

RCRA, Superfund, and EPCRA Call Center. <http://www.epa.gov/epaoswer/hotline/> (January 29, 2003).

Remote Sensing Data and Information. <http://rsd.gsfc.nasa.gov/rsd/RemoteSensing.html> (February 26, 2003).

Render Safe, Defusing a Nuclear Emergency. Los Alamos National Laboratory. Fall 2002. <http://www.lanl.gov/quarterly/q_fall02/render_safe.shtml> (March 26, 2003).

Resources for Law Enforcement. Anti-Defamation League. <http://www.adl.org/learn/additional_resources/default.asp> (April 29, 2003).

Rhode Island Department of Health: Bioterrorism Preparedness Program. "History of Biological Warfare and Current Threat." <http://www.healthri.org/environment/biot/history.htm> (March 12, 2003).

Richelson, Jeffrey T. Science, Technology and the CIA. National Security Archive, George Washington University. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB54/index2.html> (April 24, 2003).

Royal College of Pathologists. "Medical Microbiology." 2002. <http://www.rcpath.org/recruitment/microbiology.htm> (January 22, 2002).

Russian Informational Centre. Ministry for Press, Television, Radio Broadcasting and Mass Communications of the Russian Federation. <http://www.infocentre.ru/eng_user/> (April 30, 2003).

Satellite Remote Sensing. University of Waterloo Faculty of Environmental Sciences. <http://www.fes.uwaterloo.ca/crs/geog165/srs.htm> (February 26, 2003).

Schroeder, Norbert. "Radio Frequency Spectrum Allocations in the United States." National Telecommunications and Information Administration. July 1, 2000. <http://www.ntia.doc.gov/osmhome/chart_00.htm> (January 30, 2003).

Scripps Center for Mass Spectrometry. <http://masspec.scripps.edu/information/intro/index.html.> (January 5, 2003).

Security Policy Board Documents. Federation of American Scientists. <http://www.fas.org/sgp/spb/> (April 2, 2003).

September 11 Archive. <http://september11.archive.org/> (April 22, 2003).

Short, Nicholas M., Sr. "The Remote Sensing Tutorial." NASA. October 22, 2002. <http://rst.gsfc.nasa.gov/> (November 14, 2002).

Taylor, Francis X. U.S. Department of State. "Patterns of Global Terrorism 2001, Annual Report: On the Record Briefing." May 21, 2002. <http://www.state.gov/s/ct/rls/rm/10367.htm> (April 17, 2003).

Terrorism Act 2000. Her Majesty's Stationery Office. <http://www.hmso.gov.uk/acts/acts2000/20000011.htm> (April 7, 2003).

Terrorism Risk Insurance Program. U.S. Department of the Treasury. <http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/> (March 28, 2003).

Terrorism/Counter-Terrorism Web Links. United States Institute of Peace. <http://www.usip.org/library/topics/terrorism.html> (May 1, 2003).

The American Civil Defense Association. <http://www.tacda.org/> (April 11, 2003).

The Center for Counterintelligence and Security Studies. <http://www.cicentre.com> (April 2003).

Transportation Safety Administration. <http://129.33.119.130/public/index.jsp> (March 12, 2003).

"Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, 944 U.N.T.S. 13." Nuclear Age Peace Foundation. 2002. <http://www.nuclearfiles.org/docs/1972/720526-abm.html> (December 9, 2002).

U.S. Agency for International Development. <http://www.usaid.gov/> (April 25, 2003).

U.S. Air Combat Command. <http://www2.acc.af.mil/> (April 13, 2003).

U.S. Air Intelligence Agency. <http://aia.lackland.af.mil/> (April 13, 2003).

U.S. Department of Defense. <http://www.defenselink.mil/> (April 28, 2003).

U.S. Department of Homeland Security. <http://www.dhs.gov/dhspublic/> (April 10, 2003).

U.S. Department of Justice. <http://www.usdoj.gov/> (April 14, 2003).

U.S. Department of State. <http://www.state.gov/> (April 25, 2003).

U.S. Department of Transportation. <http://www.dot.gov/> (April 3, 2003).

U.S. Intelligence and Security Agencies. Federation of American Scientists. <http://www.fas.org/irp/official.html> (April 29, 2003).

U.S. Intelligence Community. <http://www.intelligence.gov/> (April 14, 2003).

U.S. Navy—The Aircraft Carriers. U.S. Navy Office of Information. <http://www.chinfo.navy.mil/navpalib/ships/carriers/> (April 13, 2003).

U.S. Nuclear Regulatory Commission. <http://www.nrc.gov/> (April 15, 2003).

United Kingdom Atomic Energy Authority. "Focus on Fusion" <http://www.fusion.org.uk/focus/index.htm> (March 29, 2003).

United Kingdom Government. The Public Record Office. <http://www.pro.gov.uk.htm> (October 17, 2002).>

United Kingdom Government. "UK government online." <http://www.ukonline.gov.uk/Home/HOHome/1,1031,~801b22~fs~en,00.html> (October 19, 2002)

United Kingdom Government, Ministry of Defence. "Defence Issues; Science and Technology." September 3, 2002. <http://www.mod.uk/issues/science.htm> (October 17, 2002).

United Kingdom Intelligence Agencies. Federation of American Scientists. <http://www.fas.org/irp/world/uk/index.html> (April 11, 2003).

United Nations. <http://www.un.org> (April 1, 2003).

United Nations. Security Council Resolution 1441. November 7, 2002. <http://www.un.int/usa/sres-iraq.htm> (March 23, 2003).

United States Air Force Special Operations Command. <http://www.afsoc.af.mil/> (April 2, 2003).

United States Air Force Wargaming Institute. <http://www.cadre.maxwell.af.mil/wargame/main.htm> (March 14, 2003).

United States Army <http://mrmc-www.army.mil/> (April 10, 2003).

United States Army Corps of Engineers Topographic Engineering Center. "TEC Web Site." 2002. <http://www.tec.army.mil/> (February 11, 2003).

United States Army Intelligence and Security Command. <http://www.inscom.army.mil> (February 2, 2003).

United States Army Medical Research Institute of Chemical Defense. <http://chemdef.apgea.army.mil/> (April 10, 2003).

United States Army Soldier and Biological Chemical Command (SBCCOM). <http://www.sbccom.army.mil/> (January 27, 2003).

United States Army Special Operations Command. <http://www.bragg.army.mil/18abn/usa_special_operations_command.htm> (April 2, 2003).

United States Chemical Safety and Hazard Investigation Board. <http://www.chemsafety.gov/about> (January 19, 2003).

United States Commission on Civil Rights. <http://www.usccr.gov> (January 29, 2003).

United States Congress 107th Congress 2nd Session. "Technology assessment in the war on terrorism and homeland security: the role of OTA" Committee Print. April 2002. <http://www.fas.org/irp/congress/2002_hr/ota.html> (December 15, 2002).

United States Department of Agriculture. "The AQI Program at Airports." <http://www.aphis.usda.gov/oa/pubs/detdog1.html> (February 20, 2003).

United States Department of Energy. *Atomic Century.* <http://www.dpi.anl.gov/dpi2/hist_docs/treaties/start2.htm.> (December 20, 2002).

United States Department of Energy, Department of Fossil Reserves. <http://www.fe.doe.gov/program_reserves.html> (March 2, 2003).

United States Department of Energy, Office of Fusion Energy Sciences. "Welcome to the U.S. Fusion Energy Sciences Program." <http://wwwofe.er.doe.gov/> (March 30, 2003).

United States Department of Energy, Office of Science. National Laboratories and User Facilities. <http://www.sc.doe.gov/Sub/Organization/Map/national_labs_and_userfacilities.htm> (March 23, 2003).

United States Department of Homeland Security. Bureau of Citizenship and Immigration Services, PORTPASS. March 11, 2003. <http://www.immigration.gov/graphics/howdoi/portpass.htm> (April 9, 2003).

United States Department of Homeland Security. Immigration Information, INSPASS. March 4, 2003. <http://www.immigration.gov/graphics/shared/howdoi/inspass.htm> (April 9, 2003).

United States Department of Homeland Security. Research &Technology. <http://www.dhs.gov/dhspublic/display?theme=27&content=374> (March 23, 2003).

United States Department of Justice. "National Drug Threat Assessment 2002." December 2001 <http://www.usdoj.gov/ndic/pubs/716/> (March 11, 2003).

United States Department of State. Annual reports. <http://www.state.gov/www/global/terrorism/annual_reports.html> (April 16, 2003).

United States Department of State. "Parties and Signatories of the Biological Weapons Convention" December 11, 2002. <http://www.state.gov/t/ac/bw/fs/2002/8026.htm> (February 25, 2003).

United States Department of State Bureau of Arms Control <http://www.state.gov/t/ac/> (December 30, 2002).

United States Department of the Treasury. <http://www.ustreas.gov> (March 17, 2003).

United States Department of the Treasury. U.S. Customs Service. <http://www.customs.ustreas.gov/>

United States Department of Transportation. "United States Coast Guard." January 27, 2003. <http://www.uscg.mil/USCG.shtm.asp> (January 27, 2003).

United States Environmental Protection Agency. "EPA's Role and Authority in Counter Terrorism" Chemical Emergency Preparedness and Prevention. <http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ct-epro.htm#epa> (February 15, 2003).

United States Federal Bureau of Investigation. <http://www.fbi.gov/libref/historic/famcases/hanssen/hanssen.htm#anchor26782> (April 2003)

United States Geological Survey. <http://www.usgs.gov> (February 13, 2003).

United States National Archives & Records Administration. <http://www.archives.gov/>

United States National Oceanic & Atmospheric Administration. <http://www.noaa.gov.> (January 15, 2003)

United States National Response Team. <http://www.nrt.org/> (March 30, 2003).

United States National Security Agency. <http://www.nsa.gov>(January 3, 2003).

United States National Transportation Safety Board. <http://www.ntsb.gov> (April 30, 2003).

United States Secret Service. <http://www.ustreas.gov/usss/> (February 5, 2003).

United States Senate Select Committee on Intelligence. <http://intelligence.senate.gov/> (April 2, 2003).

United States Strategic Command. <http://www.stratcom.af.mil/> (March 28, 2003).

University of California at Los Angeles. "Anthrax as a Weapon." College of Letters and Science. February 2002. <http://www.college.ucla.edu/webproject/micro12/m12webnotes/anthraxweapon.html> (December 29, 2002).

University of California. Southern Regional Library Facility. The history of microfilm: 1839 to present. December 3, 2002. <http://www.srlf.ucla.edu/exhibit/text/BriefHistory.htm>(March 10, 2003).

"Using and Wearing Radiation Dosimeters." Princeton University: Environmental Health and Safety. <http://www.princeton.edu/~ehs/UsingandWearingDosimetry.html> (April 17, 2003).

Vietnam War Declassification Project. Gerald R. Ford Library and Museum. <http://www.ford.utexas.edu/library/exhibits/vietnam/> (February 5, 2003).

Voice of America. "About VOA." February 1, 2003. <http://www.voa.gov/index.cfm> (February 1, 2003)

Whistleblower Disclosures. U.S. Office of Special Counsel. <http://www.osc.gov/wbdisc.htm> (April 2, 2003).

White House. "History of the National Security Council, 1947–1997." <http://www.whitehouse.gov/nsc/history.html> (April 25, 2003).

White House. "National Security." <http://www.whitehouse.gov/response/index.html> (April 27, 2003).

White House. "President's Foreign Intelligence Advisory Board." <http://www.whitehouse.gov/pfiab/;> (March 29, 2003).

White House, News & Policies. President Details Project BioShield. February 3, 2003. <http://www.whitehouse.gov/news/releases/2003/02/20030203.html> (April 3, 2003).

White House Office of National Drug Control Policy. <http://www.whitehousedrugpolicy.gov/> (February 22, 2003).

Wilkins, Gus. "The DA-Notice Website—The Official Site of the Defence, Press, and Broadcasting Advisory Committee." <http://www.dnotice.org.uk/index.htm> (December 1, 2002).

Wilson, Elizabeth. *Introduction to AMMOS Telemetry Processing.* Jet Propulsion Laboratory, NASA. October 18, 2001. <http://tel.jpl.nasa.gov/~betsy/mm/intro.htm> (November 14, 2002).

Wired News. "DNA Tagging." Stewart Taggart. <http://www.wired com/news/print/0,1294,34774,00.html> (January 15, 2003).

Woolf, Amy F. "Nuclear Weapons in the Former Soviet Union: Location, Command, and Control." Congressional Research Service Report 91144. <http://www.fas.org/spp/starwars/crs/91–144.htm> (February 28, 2003).

World Health Organization. Communicable Disease Surveillance & Response (CSR). April 24, 2003 <http;//www.who.int/csr/sars/en/> (April 27, 2003)

World Health Organization. WHO Fact Sheets, May 2003. <http://www.who.int/health-topics/zoonoses.htm> (May 12, 2003)

How to go to your page

Index

Page references include both a volume number and a page number (for example, 1:286 refers to volume 1, page 286). Boldface page references signify the location of main articles. Italic page references indicate illustrations.

A

Abbe, Ernst, 2:270
ABMT. *See* Advanced biomedical technologies program (ABMT)
ABM Treaty. *See* Anti-Ballistic Missile Treaty (1972)
Abrams, Elliott, 2:156
Abu Nidal Organization (ANO), **1:1**
Abu Sayyf Group (ASG), **1:1–2**
Abwehr, **1:2–3,** 2:64
Acambis, Inc., 3:*87*
ACC. *See* Air Combat Command (ACC)
Acheson, Dean, 1:325
Acoustic bullets. *See* Audio Amplifiers
Acoustics and acoustic devices, 1:69–70
Acoustic stealth. *See* Stealth technology
Adams, John Quincy, 1:28
ADF. *See* Allied Democratic Forces (ADF)
ADFGX Cipher, **1:3–4,** 1:205, 1:*4*
ADIO. *See* Australian Defense Intelligence Organization (ADIO)
Adleman, Leonard, 1:286
Advanced biomedical technologies program (ABMT), 1:119
Advanced Encryption Standard, 1:227, 1:228, 1:291, 1:396
Advance Passenger Information System (APIS), **1:44–45,** 3:72
Aerial photography and reconnaissance, 1:73–76, 2:59
  balloon development for, 1:92
Aeronautical and aerospace research (NASA), 2:298
AES. *See* Atomic emission spectroscopy (AES)
AFGE. *See* American Federation of Federal Employees (AFGE)
Afghanistan
  Al-Qaeda base in, 1:27, 1:149, 3:68
  Communists in, 1:196
  Operation Enduring Freedom, 1:397–398, 2:274
  Soviet invasion of, 1:240
Aflatoxin, **1:5,** 3:166
AFOSI. *See* Air Force Office of Special Investigations (AFOSI)
Africa
  European colonies in, 1:6
  U.S. security policy and interventions, **1:5–9,** 1:*6*
AFTAC. *See* Air Force Technical Applications Center (AFTAC)
Agent Orange, **1:9–10,** 1:181
AIA. *See* Air Intelligence Agency (AIA); American Institute of Architects (AIA)
AIDS
  Soviet disinformation on, 1:333
  vaccine research, 3:224
Airborne Command Post (Looking Glass), **2:237,** 2:*238*
Air Combat Command (ACC), 1:12
Air Commerce Act (1926), 2:2
Aircraft
  hypersonic and rocket powered, 2:90–92
  Identification Friend or Foe (IFF), 2:98
  intelligence gathering, 1:11–13
Aircraft carrier, **1:17–20**, 1:*18*
Air Force intelligence (U.S.), **1:11–13**, 1:*12*
Air Force Office of Special Investigations (AFOSI), **1:13–14**
Air Force Technical Applications Center (AFTAC), 1:12
Air Force (U.S.)
  Tethered Aerostat Radar System, 1:94
Air Intelligence Agency (AIA), 1:*12*
Airline security, **1:20–22**, 1:*21*
Air marshals, U.S., **1:14–16**, 1:*15*
Air plume and chemical detection, **1:16–17**
Airport security, 1:20–21
  See also Airline security
Air purification
  contamination/decontamination, **1:10–11**, 1:*10*
Airships, 1:93
  See also balloon flight
Air technical intelligence, 1:73–76
Air wings (aircraft carriers), 1:17–18
Al-Aqsa Martyrs Brigade (Palestine), **1:23**
Alaskan Pipeline, 2:384
al-Banna, Sabri, 1:1
Alberti, Leon Battista (1404–1472), 1:204, 1:227, 1:288
Albright, Madeleine, 1:325
Alcohol Tax Unit (ATU), 1:68
Alex Boncayao Brigade (ABB, Philippines), **1:23**
Al-Gama'a al-Islamiyya (Islamic Group, IG), **1:23–24**
Algorithms and data mining, 1:307
  See also Ciphers, algorithmic
Alien Registration Act (1940), 2:251
ALIR. *See* Army for the Liberation of Rwanda (ALIR)
Al-Ittihad al-Islami (AIAI), **1:24**
Al-Jama'a al-Islamiyyah al-Muqatilah bi-Libya, **1:25**
Al-Jihad, **1:25**
Al-Kindi, Abu Yusef, 1:226
Allende, Salvador, 1:29
Allied Democratic Forces (ADF), **1:26**
Al-Owhali, Mohamed Rashad Daoud, 2:200
Al-Qaeda, 1:6, **1:26–27**
  'Asbat al-Ansar funding from, 1:57
  assassinations, 1:61
  in Canada, 1:162
  capture of Khalid Sheikh Mohammed, 1:49
  intelligence on, 3:146
  September 11 attacks on U.S., 3:68, 3:270
  treatment of POWs, 2:125
  USS *Cole* incident, 3:216–217
  wanted poster for leaders of, 1:*277*
Al-Qaida. *See* Al-Qaeda
Al-Zawahiri, Aiman, 1:*277*
American Airlines

How to go to your page

hijacked flights—9/11, 3:69
LAX terminal, 1:*21*
American Civil Liberties Union (ACLU), 2:448
American Communist Party, 2:252–253
American Federation of Federal Employees (AFGE), 1:77
American Institute of Architects (AIA), 1:49
American Media Inc., 1:*40*
American Revolution
espionage and intelligence in, **3:21–23**
guerilla warfare tactics in, 2:74, 3:206
American Society of Civil Engineers
WTC tower collapse study, 1:50
Americas, modern U.S. security policy and interventions, 1:28–31
Ames, Aldrich H., **1:31–33,** 1:196, 2:280–281
Analytical chemistry, 1:183
See also Chemistry; Forensic chemistry
Anarchism ideology, 3:148
Andrea Doria (aircraft carrier), 1:20
Angleton, James, 1:*202,* 2:281
Anglo-Russian Convention (St. Petersburg, 1907), 2:72
Angola, 1:8
Animal research
adaptations and behaviors derived from genetic, 1:113
Anthropod-borne Animal Disease Research Laboratory (USDA), 1:*109*
ANO. *See* Abu Nidal Organization (ANO)
Anthrax, **1:33–34,** 2:279, 3:*214*
American Media Inc. cleanup site, 1:*40*
biodetector defense against, 1:111
as biological weapons, 1:34–37, **1:39–41,** 1:43, 2:103
biotechnology and, 1:36–37
ease of delivery, 1:36
in Iraq, 2:165
military research of, 1:36
production of, 1:36–37
reward poster, 1:*35*
spores, 3:109–110, 3:244–245
testing on Gruinard Island, 1:118
vaccine, **1:37–39,** 1:*38*
Anthropod-borne Animal Disease Research Laboratory (USDA), 1:*109*
Anti-Ballistic Missiles (ABM), 3:120–121
Anti-Ballistic Missile Treaty (1972), **1:41–42,** 3:121
Antibiotics, **1:43–44**
genomic research in, 2:57–58
National Pharmaceutical Stockpile Program (NPS), 1:126, 1:319
resistance to, 1:43, 1:81, 1:82–83, 2:265
stockpiling of, 1:125
Anti-drug campaign
Anti-Drug Abuse Act (1988), 1:362
Anti-drug advertising, 1:362
Drug-Free Communities Act (1997), 1:362
Anti-government groups (U.S.), 3:143–144
Anti-imperialist Territorial Nuclei (NTA, Italy), **1:44**
Anti-spam legislation, 2:144
Anti-Terrorism, Crime and Security Act, U.K. (2001), 2:123
Apartheid, 1:8
APIS. *See* Advance Passenger Information System (APIS)
Apollo space program
need for miniaturized electronics, 2:266
PNNL analysis of lunar materials, 2:394
Arab-Israeli wars, 2:273
Arab Revolutionary Brigades. *See* Abu Nidal Organization (ANO)
ARAC. *See* Atmospheric Release Advisory Capability (ARAC)
Arbenz Guzman, Pres. Jacobo (Guatemala), 1:29
Archeology and artifacts
changing practices of preservation, 1:46
Holocaust plunder, 1:47
wartime protection of, **1:45–48**
See also Art and antiquities
Architecture
building risk assessment software (RAMPART), 1:49
hidden security checkpoints, 1:50
structural security and, **1:48–50**
Area 51 (Groom Lake, Nevada), **1:51**
Argentina, intelligence and security, **1:51–53**
Argonne National Laboratory, **1:53,** 1:*54,* 1:111
Aristide, Pres. Jean-Bertrand (Haiti), 1:30
Armed Islamic Group (GIA), **1:54**
Arms control
Conventional Forces Europe (CFE) Agreement, 1:147
United States Bureau of, **1:55**
See also Gun control; Nuclear arms control
Arms control agreements
ballistic missiles and nuclear arsenal, 1:76, 1:89
satellite verification, 3:45
Arms Export Control Act, 2:155
Army Field Manual forgery, 1:348
Army for the Liberation of Rwanda (ALIR), **1:55**
Army Security Agency (ASA, U.S.), **1:56,** 2:209
Army Signal Intelligence Service, U.S. (SIS). *See* Signal Intelligence Service (SIS, U.S. Army)
Army Signal Security Service, U.S. *See* Signal Intelligence Service (SIS, U.S. Army)
ARPANet, 2:141
Arson investigations, ATF, 1:68
Art and antiquities
looting of, 1:45–46
Napoleonic Wars destruction of, 1:46
Nazi Germany "Great Theft," 1:47
repatriation of, 1:46
ASA. *See* Army Security Agency (ASA, U.S.)
'Asbat al-Ansar, **1:57**
ASG. *See* Abu Sayyf Group (ASG)
Ashcroft, John, 2:*318*
Asia
Britain-Russian imperialistic rivalry over, 2:70–72
IMF focus on, 2:99
Asilomar Conference, **1:57–58**
Aspin, Secretary. of Defense Les, 1:7–8
Assassination, **1:58–62**
Al-Qaeda and, 1:60–61
attempts, 1:60–61
biochemical techniques, 1:63–64
biochemical weapons, 1:106–108
electronic triggers, 1:329
history of, 1:58, 1:60–61
mechanical weapons, **1:62–65**
Astronauts, U.S., 2:299
Asymmetric warfare, **1:68**
ATF (United States Bureau of Alcohol, Tobacco, and Firearms). *See* Bureau of Alcohol, Tobacco, and Firearms (ATF)
Atmospheric Release Advisory Capability (ARAC), **1:68–69**
Atomic bomb, 2:23
Atomic emission spectroscopy (AES), 2:24
Atomic Energy Detection System (USAEDS). *See* U.S. Atomic Energy Detection System (USAEDS)
ATSA. *See* Aviation and Transportation Security Act (ATSA)
ATU. *See* Alcohol Tax Unit (ATU)
Aubisson, Roberto d', 1:30
Audio amplifiers, **1:69–70**
Aum Shinrikyo, Aleph, 1:139
use of nerve gas, 1:36, 1:40–41, 1:64, 3:*40*
See also Aum Supreme Truth (Aum)
Aum Supreme Truth (Aum), **1:71**
See also Aum Shinrikyo, Aleph
Australia, intelligence and security, **1:71–72**
Australian Defense Intelligence Organization (ADIO), 1:72
Austria, intelligence and security, **1:73**
Aviation and Transportation Security Act (ATSA), 1:14, 1:20–21, 1:77, 1:209
Aviation intelligence
Air Force intelligence, 1:11–13
history of, **1:73–76**

Aviation security
civil, U.S., **1:209–210**
NTSB accident investigations, 2:*361*
PanAm 103 bombing investigation, 2:399–400
screeners, **1:77–78,** 1:209–210
turbulence detection, 1:364

B

B-2 Bomber, **1:79**
B-52, **1:80**
Bacillus anthracis. See Anthrax
Background investigations, 1:322
Backscatter imaging, 3:53
Bacon, Roger (1220–1292), 1:227
Bacteria
aerobic and anaerobic, 1:81
DNA in, 1:80–81, **1:335–338**
identification and classification, 1:81
spore formation, 3:109–110
toxins, 3:166
treatment of, 1:83–84
viral genetics, 1:82–84, 3:237–239
Bacterial biology, **1:80–85**
Bacterial infections
antibiotics for, 1:43
antibody formation, 1:81
disease from, 1:83–84
Baghdad Pact, 1:237
Bakunin, Mikhail (1814–1876), 3:148, 3:150
Ballistic fingerprints, **1:85**
Ballistic missile defense (BMD)
boost phase intercept, 3:121–122
cruise phase intercept, 3:123
descent phase intercept, 3:123–124
Ballistic Missile Defense Organization (BMDO, U.S.), **1:86**
Ballistic missiles, **1:87–91**, 1:*87–88*
arms control agreements, 1:89, 2:30
Ghauri (Pakistan), 1:*88*
Minuteman ICBM (U.S.), 1:*87*
precision-guided, 2:*172*
proliferation of, 1:90–91
R-7 ICBM (Soviet Union), 1:89
Balloon flight
in Civil War (U.S.), 1:211
first manned flights, 1:91
Hindenburg crash, 1:93
Japanese WWII balloon bombs, 2:34
Montgolfier brothers, 1:92
See also Airships
Balloon reconnaissance, 1:*91*
Air Force aerostats (blimps), 1:94
history of, **1:91–94**
photography, 2:424–425
Project GENETRIX, 1:93–94
Bamford, James, 2:352
El Baradei, Mohamed, 2:139, 2:161
Barannikov, Victor, 1:*148*
Barre, Maj. Gen. Mohamed Siad, 1:7
Basque Fatherland and Liberty (ETA), **1:94–95**
Bathymetric maps, **1:95–96**
Batista, Fulgencio, 1:28
Battle groups (aircraft carriers), 1:17
Baudot code, 1:242, 2:21
Bauer, Edger (1820–1886), 3:148, 3:150
Bay of Pigs, **1:96–98,** 1:293
Brigade 2506, 1:97–98
BayTSP
copyright laws and, 1:272
Beckwith, Byron De La, 2:8
Beckwith, Col. Charles, 1:322
Belgium, intelligence and security, **1:98–99**
Belly buster hand drill, **1:99**
Ben-Gurion, David, 2:283
Berlin Airlift, **1:99–101,** 1:*100*
operations, 1:100–101
Berlin refugees, 1:103–105
Berlin Tunnel, **1:101–103,** 1:*102*
Berlin Wall, 1:101, **1:103–106**
Brandenburg Gate, 1:*104*
building of, 1:105–106
Checkpoint Charlie, 1:*236*
fall of, 1:106, 1:*239,* 1:241
Berman, Howard L., 3:42
Berners-Lee, Tim, 1:171–172, 2:142
Bernstein, Carl, 1:202
Bernstorff, Count Johann Von, 1:130
Bethe, Hans, 2:246
Bethe carbon cycle, 2:44–45
Bigliarrdo, Roberto Felice, 1:*371*
Bill of Rights, 2:447
Bin Laden, Osama, 1:6, 1:*277*
al-Qaeda, 1:26, 1:149
'Asbat al-Ansar, 1:57
September 11 attacks on U.S., 3:270
Biochemical assassination weapons, **1:106–108**
cyanide, 1:107, 1:298–299
decontamination from, 1:317–318
detection devices for, 1:143
hemlock, 1:106
poison firing devices, 1:63–64, 1:65, 1:*107*
ricin, 1:107, 3:24, 3:166–167
Sidney Gottlieb and the CIA, 1:108
VX nerve agent, 3:246–247
Biocontainment laboratories, **1:108–110,** 1:*109,* 3:215
Biodetectors, **1:110–111**
Bio-engineered tissue constructs, **1:111–112**
Bio-flips, **1:112**
Bioinformatics, 2:57
Biological and biomimetic systems, **1:113**
Biological and Toxin Weapons Convention, **1:113–114,** 1:116
Biological input/output systems (BIOS), **1:114–115**
Biological systems
biodetectors, 1:110–111
bio-flip implants for monitoring, 1:112
biomimetic systems, 1:113
Bio-Optical Synthetic Systems (BOSS), 1:121–122
biosensors, 1:117
BioShield Project, 1:122–123
DNA implants into microorganisms, 1:114–115
Life Support for Trauma and Transport (LSAT), 1:120
Personal Status Monitor (PSM), 1:119–120
Biological warfare, **1:115–116**
advanced diagnostics, **1:117**
anthrax and, 1:33–34, 1:34–37
biodetectors as defense from, 1:110–111
bioterrorism and, 1:123–125, 2:103
deterrence strategies to biological warfare, 1:125–126
as security threat, 2:264–265
technology for, 1:174
Biological weapons
aflatoxin, 3:166
air, food and water contamination, 1:10–11, 2:29
anthrax, 1:33–34, 1:34–37, **1:39–41,** 1:43
Aum Shinrikyo (Japanese cult), 1:36, 1:40–41, 1:64
Biological and Toxin Weapons Convention, 1:113–114
destroyed in Iraq, 1:*115*
detection of, 1:113
development programs, 1:115–116
diplomatic control of, 1:116
genetic identification of, **1:117–118,** 1:342, 2:278–279
infectious diseases as, 1:124, 2:103
Soviet Union test facility, 3:244–245
testing of, 1:118
as weapons of mass destruction, 3:258
zoonoses, 3:286–287
Biology
bacterial, 1:80–85
Bergy's Manual, 1:81
viral, 1:81–82, 3:236–240
viral classification, 3:236–238
Bio-Magnetics, **1:119**
Biomedical technologies, **1:119–120**
BioShield Project, 1:122–123
Biometrics, **1:120–121**
Biomimetic systems, 1:113
Bio-Optic Synthetic Systems (BOSS), **1:121–122**
BIOS. *See* Biological input/output systems (BIOS); Biological systems
Biosafety level laboratories (BSL), 1:108–110
Biosensor technologies, **1:122**
bio-flip implant research, 1:112

detecting biological weapons, 1:117
tissue-based, 3:163
BioShield Project, **1:122–123**
Biotechnology
diagnostic devices, 1:117, 1:*120*
LBL research in, 2:224
nanotechnology applications in, 2:295
vaccine development, 1:143
Biotechnology programs
detection technologies, 1:110–111, 1:119
Bioterrorism, **1:123–125**
Aum Shinrikyo (Japanese cult), 1:36, 1:40–41, 1:64
biological agents and, 1:34–37, 1:*124*
bioterrorism initiative, 1:126
Bioterrorism Preparedness and Response Program (BPRP), 1:126
CDC disease surveillance as deterrence, 1:170
protective measures, **1:125–127,** 2:29, 2:435
Bishop, Pres. Maurice (Grenada), 1:29
Bjerkness, Vilhelm, 2:256
Black chamber, **1:127–128**
Black ops, **1:128**
Black September, 1:1, 1:61–62, 2:283–284
See also Abu Nidal Organization (ANO)
Black Tom explosion, **1:128–130,** 2:6
Blair, Tony (U.K. Prime Minister), 2:167–168
Blake, George (British double agent), 1:102
Bletchley Park, **1:131–133**
bombe deciphering machine, 1:131
British cryptology operations and cipher school, 1:131–133, 2:21
Cairncross and, 1:154
Colossus computer, 1:*132,* 1:138, 1:206, 1:242, 2:21, 3:185
Enigma cipher machine, 1:405–407
MI6 cryptanalysis and, 2:262
Operation Ultra, 3:184–185
tight security at, 1:132, 3:184–185
Blix, Hans, 2:163, 2:164, 2:166, 2:176
Bludgeons and blunt instruments, 1:64
Blunt, Anthony, 1:153–154
BMDO. *See* Ballistic Missile Defense Organization (BMDO, U.S.)
Bohr, Neils, 2:246, 2:294
Bolivia, intelligence and security, **1:133**
Bolland Amendment (War Powers Act), 1:30
Bolshevik-German conspiracy forgery, 1:345–346
Bomb
canine substance detection, 1:163–165
detection devices, **1:135–136**
e-bombs, 1:369–370, 1:384
JDAM, 2:187–188
Bomb damage, forensic assessment, **1:134**
Bombe, 1:131, **1:136–138,** 1:206
See also Bletchley Park
Bonaparte, Charles, 2:6
Bonaparte, Napoleon, 2:296–298, 3:127
British assassination attempts on, 2:297
Booster rockets, 1:90
Border and Transportation Security, DHS Directorate of (BTS), 1:44–45, 2:440
Border Patrol, U.S., 2:*94*
fingerprint identification systems, 2:19, 2:95
INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System), **2:115–116**
Port Passenger Accelerated Security System (PORTPASS), **2:439–440**
Border security
Border Patrol, U.S., 2:*94*
Customs Service, U.S., 1:296–297
International Border Interdiction Training, 1:*297*
Bosnia and Herzegovina
intelligence and security, **1:138–139**
NATO Stabilization Forces in, 1:138
Botulinum toxin, **1:139**
Botulism. *See* Botulinum toxin
Boyd, Belle, 1:211–212, 1:*416*
Bracy, Arnold, 3:75
Brady, James, 3:*56*
Brain-machine interfaces, **1:140**
Brain wave scanners, **1:141**
Brazil
aircraft carrier development, 1:19
intelligence and security, **1:141–142**
Brenner, Sydney, 2:53
Brezhnev, Leonid (Soviet president), 1:*166*
death of, 1:240
Soviet economy, 1:239–240
Strategic Arms Limitation Talks (SALT), 1:238
Brigade 2506 (Bay of Pigs,Cuba), 1:97–98
British Columbia Cancer Agency
SARS genome sequencing, 1:250
British intelligence
Cambridge University Spy Ring, 1:151–155
cryptology operations and cipher school, 1:131–133
MI5 (British Security Service), 2:260–261
MI6 (British Secret Intelligence Service), 2:262
Profumo affair with Soviet informant, 1:154
Room 40 cryptography (WW I), **3:28**
British Terrorism Act, **1:142**
Broglie, Louis de, 2:271, 2:295
Brookhaven National Laboratory, **1:143–144**, 1:*143*
Mini-Ramen LIDAR System (MLRS), 1:143
Brown, Ron, 1:246
Brzezinski, Zbigniew (U.S. security advisor), 1:7, 1:166, 2:358
BTS. *See* Border and Transportation Security, DHS Directorate of (BTS)
Bubonic plague, **1:144–145,** 2:279
Bucher, Lloyd M, 2:456
Budget and Accounting Act (1941), 2:48
Bugs (microphones) and bug detectors, **1:145–147**
Egyptian embassy, 1:404–405
noise generators, 2:341
parabolic microphones, 2:403
wiretaps and surveillance act restrictions, 2:31–32
See also Listening devices
Bundy, McGeorge, 2:189, 2:198, 2:358
Bureau of Alcohol, Tobacco, and Firearms (ATF), **1:66–68**
ballistic fingerprint matches, 1:85
bomb damage assessment, 1:134
Bureau of Arms Control (U.S.), **1:55**
Biological and Toxin Weapons Convention, 1:113
Bureau of Diplomatic Security, U.S., **1:330**
Bureau of Industry and Security, U.S. (BIS), 1:246
Bureau of Intelligence and Research (INR) U.S. State Dep't, **1:323–324**
Burgess, Guy, 1:153
Bush, George H.W.
as CIA director, 1:196, 1:310
Panama intervention, 1:30, 1:279
Persian Gulf War, 1:147
U.S. and Russia announces testing moratorium, 1:254
Bush, George W., 1:*194*
Antiballistic Missile (ABM) Treaty, 1:*42*
at Argonne National Laboratory, 1:*54*
BioShield Project, 1:123
national security policy, 1:148–150
9/11 terrorist attacks, 1:148, 3:70–71
United Nations and Iraq disarmament, 2:163–167
Voice of America, 3:*243*
war on terrorism, 3:71–72
Bush administration (1989–1993)
National Security Council, 2:358–359
National Security Directive, 1:147
national security policy, **1:147**
Somalian relief and Mogadishu debacle, 1:7–8
Bush administration (2001-)
Antiballistic Missile (ABM) Treaty, 1:*42*
National Security Council, 2:359
national security policy, **1:148–150**
2002 National Security Strategy, 2:310–311

pre-emptive strike doctrine, 1:149–150
Saddam Hussein and Iraq, 2:166, 2:173–176
war on terrorism, 1:279, 3:71–72

C

Cadore letter forgery, 1:344
Cailliau, Robert (WWW co-creator), 1:171–172
Cairncross, John, 1:154
Caller ID, **3:137–138**
Cambodia
communist capture of the Mayaguez, 2:30
Freedom Fighters, **1:151**
Cambridge University Spy Ring, **1:151–155,** 2:203, 2:261, 3:96
defections of, 1:153
Michael Straight and Anthony Blunt, 1:154
Cameras, **1:155–157**
concealment of, 1:157–158, 1:265–266
copy, 1:156–157
digital, 2:423
disguising, 1:159
infra-red, 1:390
miniature, **1:157–160,** 1:265–266
robot camera (German), 1:156
Camouflage and concealment
concealment devices, 1:265–267, 1:*266*
passive methods, 1:157–158, 1:265
Canada
Canadian Security Intelligence Agency (CSIS), 1:160, 1:161–163
counter-terrorism policy, **1:160–161**
intelligence and security, **1:161–163**
NORAD (North American Air Defense Agreement), 2:344–346
October Crisis of 1970, 1:160
Resolution 1373 (U.N. Security Council), 1:160–161
Royal Canadian Mounted Police (RCMP), 1:161, 1:363
terrorism in, 1:160, 1:162
Canaris, Wilhelm, 1:2–3, 2:64
Canine substance detection, **1:163–165**
Carcinogens, 1:5, 3:166
Carlucci, Frank, 2:358
Carroll, Joseph, 1:13
Car security, LoJack and GPS, 2:*69*
Carter, James E., 1:*166,* 1:*167*
CIA surveillance restrictions, 1:203
Iranian hostage crisis, 1:166
Shah of Iran and hostages, 2:159–160
Somalia agreements, 1:7
Carter administration (1977–1981)
cut aid to dictatorships, 1:29
National Security Council, 2:357–358
national security policy, **1:165–167**
openness policy, 1:279
Somalia agreements, 1:7
Casey, William J., 1:196, 1:311
Castilla Armas, Carlos, 1:29
Castro, Fidel, 1:28, 1:29
Bay of Pigs, 1:96–98, 1:293, 2:198
CIA disruption attempts, 2:387–388
Soviet missile deal (missile crisis), 1:293–295
CBIRF. *See* Chemical and Biological Incident Response Force (CBIRF)
Census Bureau, 1:245–246
Center for the Study of Intelligence (CSI, CIA), **1:196–197**
Centers for Disease Control and Prevention (CDC), **1:168–170,** 2:455
branch of HHS, 2:81
cost study of disease outbreaks, 2:104
economic and bioterrorism report, 1:36
protective measures development, 1:126
SARS genomic map, 1:250
Central Asia
Britain-Russian imperialistic rivalry over, 2:70–72
CERN, **1:170–172**
Berners-Lee and the World Wide Web, 1:171–172, 2:142
particle physics and accelerators, 1:170–*171*
Chad, oil revenue economic controls, 1:9
Chadwick, Sir James, 2:*246*
Chamora, Violeta, 1:30
Charged coupling devices (CCD), 2:422
Charles de Gaulle (aircraft carrier), 1:20
Charles' Law (atmospheric gases), 2:258
Chechen-Russian conflict, **1:172–173**
Chechnya (Russian republic), 1:172–173
Russian-Chechen referendum, 1:173
Russian troops in, 1:173
Stalin's mass deportation from, 1:172
Chemical analysis, 1:184–185
Chemical and Biological Defense Information Analysis (CBIAC), **1:174**
Chemical and Biological Incident Response Force (CBIRF), **1:176–177,** 1:*179*
Chemical and Biological National Security Program (CBNP), 2:339–340
Chemical and biological science and technology
analysis of manufacturing processes, 1:174
detection technologies, **1:175–176**
Chemical-biological mass spectrometer (CBMS), 2:179, 2:381
Chemical Safety and Hazard Investigation Board (USCSB, U.S.), **1:177–178**
Chemical safety and response
accidental release of chemicals, 1:177
Chemical and Biological Incident Response Force (CBIRF), 1:176–177, 1:*179*
Chemical Safety and Hazard Investigation Board (USCSB, U.S.), 1:177
decontamination, 1:316–318
detection technologies, 1:175–176
emergency responses, **1:178–179**
federal assistance, 1:179
state and local emergency response commissions, 1:178–179
Chemical warfare, **1:180–183**
chemical agents used, 1:181–183, 2:321–322
Chemical and Biological Incident Response Force (CBIRF), 1:176–177
radiological, 1:171
Chemical warfare response teams, 1:*182*
Chemical and Biological Incident Response Force (CBIRF), 1:176–177
Chemical Biological Incident Response Force (U.S. Marines), 1:176–177
Chemical weapons
Geneva Protocol (1925) ban on, 1:180–181
Iraq's use of, 1:176, 1:298, 1:319, 2:165
mustard gas, 2:290–291
nerve gases, 2:321–322
in Vietnam war, 1:*181*
as weapons of mass destruction, 3:258
in World War I, 1:180–181, 3:272–273
Chemistry
analytical, 1:183
applications for intelligence community, **1:183–185**
forensic, 1:183, 1:338, 2:37
separation methods, 1:183–184
Chernobyl nuclear power plant accident, **1:185–188,** 1:*186,* 2:24
satellite imagery of, 1:187
Chiang Kai Shek (Taiwanese leader), 1:233, 3:134
Children's Television Act, 2:10
Chile
aircraft carrier development, 1:19
intelligence and security, **1:188–189**
intervention in, 1:29
political dissidents treatment in, 1:188
China
aircraft carrier development, 1:19–20
censorship in, 1:190
civil war in, 1:233
formation of People's Republic of China (PRC), 2:208
intelligence and security, **1:189–190**
looting of historical artifacts, 1:46
Nixon's visit to, 2:335
Severe Acute Respiratory Syndrome (SARS), 1:248–252

Tachen Straits crisis, 1:237
United Nations Security Council and, 1:189
U.S. satellite technology exports to, 3:41–42
U.S. warhead designs in, 1:190
Chinese espionage
Cox Report (U.S.), 1:191
interest in U. S. technology, 1:191, 1:365, 2:133
in U.S., **1:190–191**
Cholana Kangtoap Serai Cheat Kampouchea. *See* Cambodia, Freedom Fighters
Christopher, Warren, 1:217
Chromatography, 1:184
gas, 1:175, 2:38
thin layer, 2:38, 3:161–162
Church, Sen. Frank (U.S.), 1:62, 1:*107,* 1:192, 1:201, 1:203, 3:66
Church Committee, 1:*107,* **1:192–193,** 1:194
CIA legal restrictions, 1:201, 1:203, 1:279
congressional oversight of intelligence community, 1:194, 2.135–136
surveillance act passed following report, 2:31
Churchill, U.K. Prime Minister Winston, 1:231, 1:233, 3:106
CIA administration
authority lines and directorates, 1:195, 3:203
directors (DCI), 1:308–312, 3:203–204
funding for data mining research, 1:307
intelligence for U.S. President, 2:444–445
legal restrictions on, **1:202–203,** 1:279
CIA (Central Intelligence Agency), **1:193–196,** 3:*203*
assassination attempts and restrictions, 1:62, 1:194, 1:203
Bay of Pigs (Cuba), 1:293
Berlin Tunnel, 1:101–103
careers in, 2:119–120
Cold War operations, 1:232
double agents, 1:31–33, 1:102, 1:360–361
George H.W. Bush, Director of, 1:147
Project GENETRIX canceled, 1:94
publication of training manuals, 1:30
response to spy ring defections, 1:154
Sidney Gottlieb and biochemical weapons, 1:108
CIA covert operations, 1:*277*
Delta Force, Middle East and, 1:323
dirty tricks, 1:331
Glomar Explorer -Soviet submarine salvage, 2:66–67
Iran-Contra affair, 1:30, 1:279, 2:155–157
Operation Mongoose (Cuba), 2:387–388
secret Asian wars, 1:196
training and indoctrination for, 1:277–278
in Vietnam War, 1:279
Watergate break-in, 1:202
CIA directorates and services, 1:201, 1:311
Center for the Study of Intelligence (CSI), **1:196–197**
Directorate of Science and Technology (DS&T), **1:197–198**
Foreign Broadcast Information Service, **1:198–199**
guerilla warfare training base, 1:234
CIA formation and history, 1:195–196, **1:199–201,** 1:*200*
growth of, 1:200–201
CIA Information Act (1984), 1:203
CIAO. *See* Critical infrastructure Assurance Office (CIAO)
CIG (Central Intelligence Group), 1:200
CIPA. *See* Classified Information Procedures Act (CIPA)
Cipher disks and wheels, **1:204,** 1:205
in Civil War (U.S.), 1:211
Cipher keys, **1:204–205**
algorithmic, 1:218, 1:225, 1:286–287, 1:319
mobile phone, 2:73
public, 1:227–228
RSA algorithm, 1:287–288, 1:291, 2:446
Cipher machines, **1:205–207**
Colossus computer, 1:*132,* 1:138, 1:206, 1:242, 2:21, 3:185
digital computers as, 1:206
Egyptian embassy cipher room bugged, 1:404–405
Geheimschrieber, 1:205–206, 2:21
one-time tape system, 1:207
Playfair system, 1:289, **2:426**
Purple machine (Japanese), 2:459–460, 3:185
rotor-based Enigma type, 1:205, 1:*206*
Signal Intelligence Service (SIS, U.S. Army), 1:243–244, 2:386–387
Typex, **3:177**
See also Cryptography
Cipher pad, **1:207–208,** 1:291
Ciphers
ADFGX Cipher, 1:3–4, 1:205, 1:290
algorithmic, 1:218, 1:225, 1:228, 1:286–287
block, 1:227
Lorenz cipher, 1:137, 1:242, 2:21
Polybius square, 1:3–*4,* 1:288
public key, 1:227–228
stream ciphers, 1:208, 1:227
substitution cipher, 1:205, 1:226, 1:405
SZ42 Cipher, 1:205
See also Cryptography
CIPRIS. *See* Coordinating Interagency Partnership Regulatiing International Students (CIPRIS)
Civil defense
homeland security and, 2:85–86
Civil Liberties Act (1988), 2:122
Civil rights and liberties
Habeas Corpus Act (1863), 2:121–122
Patriot Act and, 1:386–387
Soviet propaganda prompted civil rights legislation, 2:450
Civil Rights Commission, U.S., **1:247–248**
Civil rights movement
Civil Liberties Act (1988), 2:122
Civil Rights Act (1957), 1:247, 2:7–8
COINTELPRO illegal operations discrediting groups, 1:229–230
FBI investigation of assassinations, 2:8
Civil War (U.S.)
Balloon reconnaissance, 1:91, 1:92
cipher disk used in, 1:204
espionage and intelligence in, **1:210–212,** 3:206–207
uncontrolled borders, 1:210
women spies in, 1:211
Clark, John (18th century), 3:22
Clark, William, 2:358
Clarke, Richard (security advisor), 1:*299*
Classified information, **1:213–216**
access to, 3:60–61
declassification of, 1:215–216
Classified Information Act (1980), 2.135
Classified Information Procedures Act (CIPA), 1:213–214, 1:259
Classified National Security Information Act, 1:214–215
Clean Air Act
1990 amendment, 1:177
Cleopatra (Egyptian Queen), 1:106
Clifford, Clark, 2:189, 2:355
Clinton, William J., 1:17, 1:*217*
Haiti intervention, 1:30
ISAC concept by, 1:301
signs Comprehensive Test Ban Treaty (CTBT), 1:254
Vietnam War influence on, 1:216–217
Clinton administration (1993–2001)
alleged Chinese campaign donations to, 1:190, 3:41
counter-terrorism policy, 1:176, 3:145–146
declaration against terrorism after Khobar Towers bombing, 2:204
foreign aid policy, 1:217
National Security Council, 2:359
national security policy, **1:216–218**
openness policy, 1:279

Presidential review directive (PRD), 1:217
U.S. satellite technology exports to China, 3:41–42
Clipper chip, **1:218**
Closed circuit television systems (CCTV), 1:156, **1:219–221**
Cloud seeding, 2:257, 2:259–260
Coast Guard, U.S., **1:221–222**
coordinating gov. agencies roles in homeland security, 1:222
National Maritime Intelligence Center, 2:336–337
National Response Center, **1:223**
National Response Team, 2:306–307
port security, 2:437–438
Port Security Units (PSUs), 2:438
Cockpit voice recorders, 2:26
Code-breakers, 1:127–128
Code names, **1:223–224**
Codes and ciphers, **1:224–228**
in American revolution, 3:22–23
code types, 1:227, 1:242
fast and scalable scientific computation of, **1:228–229**
French resistance coded messages, 2:42–43
German code books captured by British, 3:274–275
Morse code, 1:*225*
See also Ciphers
Code-talkers (Navaho Indians), 1:291, 3:263–265
Code words, **1:224**
CODIS. *See* Combined DNA Index System (CODIS)
Coherent scattering, 3:53
COINTELPRO, 1:229–230
Colby, William E., 1:*192,* 1:196, 1:310
Cold fusion, 2:45
The Cold War
aerial reconnaissance in, 1:75–76
beginnings of, **1:230–232**
Berlin blockade by Soviet Union, 1:99–101, 1:103
Berlin Wall, 1:103–106, 1:*239,* 1:241
capitalism *vs.* socialism, 1:232, 1:233
Cold War History Project, 1:332–333
development of CIA in, 1:200
end of, 1:241
KGB operations during, 2:201
Nixon's arms reduction talks, 1:238
Pres. Truman on, 1:231–232
The Cold War (1950–1972), **1:233–238**
The Cold War (1972–1989): the collapse of the Soviet Union, **1:238–241**
Colladen, Daviel, 3:90
Colombia, intelligence and security, **1:241–242**
Colossus computer (1rst programmable computer), 1:*132,* 1:138, 1:206, **1:242–243,** 2:21, 3:185
Combat aircraft
B-2 Bomber, 1:79
B-52 Bomber, 1:80
balloons use as, 1:92–93
F-117, 2:1, 3:116
in Soviet Union, 1:75
Combined DNA Index System (CODIS), 1:*336*
Commerce Department , U.S. (DOC)
Critical infrastructure Assurance Office (CIAO), 1:282–283
intelligence and security, **1:245–246**
Commissar Order (Nazi Germany), 1:3
Communicable diseases
Federal quarantine legislation, 1:250
isolation and quarantine, **1:248–252**
Communication satellites, 1:364
Communications Satellite Act, 2:10
licensing of, 3:42
Communications intelligence (COMINT), **1:243–244**
telegraph intercepts during Spanish-American War, 3:102–103
Communications policy
Children's Television Act, 2:10
Communications Act (1934), 2:10
Communication systems
diplomatic secure international, 1:252
national security and emergency preparedness, **1:252**
Communism
in African countries, 1:7–8
American Communist Party, 2:252–253
anti-communism hysteria, 2:122–123
Cold War infiltration of, 1:233
FBI domestic efforts against, 2:7
Middle East—U.S. defense against, 1:237
U.S. Communist Party and Palmer raids, 2:122
U.S. resistance to, 1:201, 1:279
Comprehensive Nuclear Test Ban Treaty Organization, 1:254
Comprehensive Test Ban Treaty (CTBT), **1:253–254,** 2:394, 3:64
ratification of, 1:254
Compton, Arthur H., 1:370
Compton effect (EMP), 1:370
Computer Abuse and Amendments Act (1994), 1:256
Computer-aided design (CAD), 1:259
Computer Assisted Passenger Prescreening System (CAPPS), 2:123–124, 3:72
Computer Conservation Society (U.K.)
preservation of Colossus cipher computer, 1:*132,* 1:138, 1:206, 1:242, 2:21, 3:185
Computer crimes
cyber-security Enhancement Act (2002), 1:256
hackers and, 1:255–256, 1:256–257
Pentagon attack, 1:256
Computer data and documents
access authorization for, 1:263
backups for security, 1:300
degausser, 1:343
digital signatures, 1:262
Computer Fraud and Abuse Act (1986), **1:255–256,** 2:302
Computer hackers, **1:256–257**
exposing computer security flaws, 1:256–257, 1:300
Computer hardware
security of, **1:257–258**
supercomputers, 3:128
theft prevention, 1:262
Computer keystroke recorder, **1:258–259**
Computer modeling, **1:259–260**
Computer networks
Echelon, 1:370–372
wireless, 1:300
Computer Security Act (1987), **1:261**
Computer Security Division (NIST), **2:333–334**
Computer software
anti-virus, 1:261–262, 2:105
building risk assessment software (RAMPART), 1:49
data encryption, 1:262, 1:289, 1:291
data mining, 1:307
Image processing, 3:13–14
Internet surveillance, 2:146
modeling, 1:259–260
name recognition, 2:94
Pretty Good Privacy (PGP), 1:228, 1:287, 1:291
security of, **1:261–263**
simulations and war games, 1:259–260
virtual reality modeling language (VRML), 1:259
Computer systems
Computer Security Act (1987), 1:261
data destruction, **1:255**
firewall software for, 1:263, 1:300
fraud and abuse of, 1:255–256
hardware security, 1:257–258
local networks, 1:258
new technologies, 3:128
security, 1:256–257, 2:8
Computer tomography (CT scanners), 1:22, 1:135–136, 3:52
Computer viruses, **1:263–265**
anti-virus software and, 1:261–262, 2:105
hackers and, 1:256, 1:300
ILOVEYOU virus, 1:*263,* 1:264
macro viruses and malicious data, 2:245
NIPC and "Love Bug" virus, 2:112–113
trojan horse programs, 1:300
Concealment devices, **1:265–267**
doo transmitter, 1:359
Congo
civil war, 1:6

How to go to your page

Congress, U. S.
Joint House-Senate Intelligence Committee, 2:*129*
oversight of intelligence community, 2:130, **2:135–136**
See also Church Committee; Pike Committee
Conner, R.D.W., 2:300
CONPLAN (counter-terrorism policy), 3:145–146
Constitutional law and privacy rights, 2:447–448
Consumer Information Center, 2:51
Consumer Product Safety Act (1972), 1:267
Consumer Product Safety Commission (CPSC), **1:267,** 1:*268*
Consumer Sentinel Network, 2:97
Contamination / decontamination
air and water security issues, 1:10–11
See also Decontamination methods
Continuity Army Council, 1:267
Continuity Irish Republican Army, **1:267–268**
Continuity of Government (U.S., COG), **1:269–270**
Department of Homeland Security changes to, 1:269–270
Mount Weather, 2:285–286
Continuous Assisted Performance (CAP), **1:270**
Coordinating Interagency Partnership Regulatiing International Students (CIPRIS), 2:114
Coordinator for Counter-Terrorism, (U.S Dept. of State), **1:270–271,** 1:*271*
COPS (Community Oriented Policing Services), 2:194, 2:221
Copyright laws
BayTSP and, 1:272
Copyright Act, U.S., 1:271
Digital Millennium Copyright Act (DMCA), 1:*272*
security, **1:271–272**
Coral Sea, battle of the, 1:19
Corporate espionage, 1:255–256
Cospass-Sarsat satellite system (NOAA), 2:341
Counter-espionage
economic espionage, 1:373
U.S. and U.K. response to spy ring, 1:154
Counterfeit currency
Counterfeiter profiles, 1:273
technology and manufacture of, 1:*273,* 1:273–274
technology preventing, 1:274
Counterfeiter profiles, 1:273
Counter-intelligence, **1:274–275**
agents, 1:*275*
CIA and, 1:194
COINTELPRO, 1:229–230
double agents, 1:275
FBI measures for, 2:7, 2:8
National Counterintelligence Policy Board, 1:324
NCIX office, 2:317–318
procedures investigation, 1:32–33
Counter-intelligence Center (CIC, CIA), 1:274
Counter-measures
electronic, 1:387–388
Counter-terrorism
CONPLAN, 3:145–146
Counter-terrorism agencies
Coordinator for Counter-Terrorism, (U.S), 1:270–271, 3:200–201
Counter-terrorism Rewards Program, 1:*276,* 1:*277*
DCI Counter-terrorist Center, 3:201
Security, Infrastructure Protection and Counter terrorism, U.S. National Coordinator, 3:62
Special Operations Command, 3:200
Counter-terrorism efforts
Austrian financial intelligence, 1:73
biodetectors, 1:110–111
Brookhaven National Laboratory, 1:143–*144*
CIA and, 1:201
FBI and, 2:8–9, 3:201
Los Alamos National Laboratory and, 2:240–241
Special Elite Anti-terrorism Force (Bolivia), 1:133
Terrorist Threat Integration Center, 1:149
Counter-terrorism operations
Argonne National Laboratory, 1:53
Delta Force, 1:322–323
Operation Liberty Shield, 2:385–386
Sudan and Afghanistan attacks, 2:274
Counter-terrorism policy
Clinton and, 1:176
deterrence, 3:199–200
food supply protection, 2:29
United States, 3:198–201
Counter-terrorism Rewards Program, **1:276**, 1:*277*
part of Rewards for Justice Program, 1:*276*
Covert operations, **1:276–279**
dirty tricks, 1:331
training and indoctrination for, 1:277–278
CPSC. *See* Consumer Product Safety Commission (CPSC)
Cray, Seymour, 3:128
Cray supercomputers, 3:128
Crib analysis, **1:280**
Crick, Francis, 2:53
Crime prevention
intelligence agencies aiding, **1:280–281**
liberal democracies and crime rate, 1:281
Crime rate trends, 2:194–195
Criminal Investigation Division (IRS), 2:138
Criminal profiling, 2:449
Crisis Relocation Facilities, 1:269
Critical infrastructure, **1:282**
Critical infrastructure Assurance Office (CIAO), **1:282–283**
Information Security, U.S. Office of, 2:106
Croatia, intelligence and security, **1:284**
Cruise missiles, **1:284–285**
Cryptanalysis
Arab invention of, 1:226–227, 1:288
breaking of Japanese naval codes (WWII), **3:285–286**
crib, 1:280
methods of, 1:228
NSA involved in, 2:352–353
Signal Intelligence Service (SIS, U.S. Army), 1:243–244, 2:386–387
use in Korean war, 2:209
Cryptography
cipher machines, 1:205–207
codes and ciphers, 1:224–228, 1:395
declassified documents, 1:216
DNA encoding, 1:341–342, 2:265
information security, 2:105–106
number theory and, **1:286–287**
quantum, 1:208, 1:228, 2:295, 2:462
stream-cipher technique, 1:205
See also Cipher machines; Ciphers; Codes and Ciphers
Cryptography computers and software
Colossus computer (1st programmable computer), 1:*132,* 1:242–243
computer simulations, 1:228–229
Pretty Good Privacy (PGP), 1:228, 1:291
scalable algorithms, 1:229
See also Cipher machines
Cryptography history, **1:287–291,** 1:*288,* 1:*289*
in American revolution, 3:22–23
Arab scholars and, 1:226–227, 1:288
black chamber and code-breakers, 1:127–128
in Civil War (U.S.), 1:211, 1:289
Egyptian hieroglyphics, 1:288
Enigma cipher machine, 1:131–132, 1:205, 1:*206,* 1:291, 1:405–407
Geheimschrieber cipher machine (WWII Germany), 1:205–206, 2:21
radio's influence on, 1:290
telegraph and, 1:419
in World War I, 1:290–291, 3:28, 3:272
in World War II, 3:281
Cryptonyms, **1:291–292**
CTBT. *See* Comprehensive Test Ban Treaty (CTBT)
CT scanners, 1:22, 3:*52*
Cuba, 1:29, **1:293–295**
CIA activities in, 1:201
independence of, 1:28

intelligence and security, **1:292–293**
Soviet signals intelligence in Lourdes, 3:*95*
Spanish-American War, 3:101–103
Cuban Missile Crisis, **1:293–295**
Kennedy communications during, 1:252
missile site in, 1:196, 1:*294*
operations against U.S., 1:292
Cult of Assassins, 1:60
Currency, U.S., 3:*170*
monetary policy and supply, 2:12–13
printing of, 1:403–404
Customs Service, U.S., **1:296–297**
Operation Green Quest, 1:296
Project Shield America, 1:296–297
CWIN. *See* Cyber Warning Information Network (CWIN)
Cyanide, 1:107, **1:298–299**
Cyber security, **1:299–301**
breaching of, 1:300–301
Cyber-security Enhancement Act (2002), 1:256
Cyber Security Research and Development Act (2002), 1:299
Cyber Warning Information Network (CWIN), **1:301–302**
Czechoslovakia
communism in, 1:232
intelligence and security, **1:302–303**

D

D notice (defense notice), **1:305**
Daley, William, 1:246
Dancer, John, 2:267
Daniken, Erik von, 2:453
DARPA (Defense Advance Research Projects Agency), **1:305–306**
Advanced Diagnostics Program, 1:117
ARPA computer network, 1:252, 1:306, 2:141
biomedical programs, 1:113, 1:114–115, 1:119–120
biotechnology programs, 1:119, 1:121–122, 1:122
brain-machine interfaces for robotics, 1:140
Continuous Assisted Performance (CAP), 1:270
Internet, dynamic and static addresses, **2:143**
rover race, 1:306
space research programs, 1:306
tissue engineering, 1:111–112
Daschle, U.S. Sen. Tom, 1:*214*
Data encryption, **1:395–396**
software, 1:262, 1:289, 1:291
Data Encryption Standard, 1:207, 1:289, 1:291, 1:396
Data mining, **1:307–308,** 1:*308*
Dead drop spike, **1:315**
Dead letter box, **1:315–316**
Debs, Eugene V. (1855–1926), 2:122
Decontaminants, 1:317–318
Decontamination methods, **1:316–319,** 1:*317*
chemical methods, 1:317–318
detoxification from mustard gas, 2:291
gaseous treatments, 2:244–245
military treatment facilities, 1:317–318
physical methods, 1:316–317
radiation, 2:244
ultra-high pressure sterilization, 2:244
U.S. mail, 2:244–245
Decryption, **1:319–320**
Bletchley Park and, 1:131–133
See also Cryptanalysis
Defense industry simulations from entertainment industry, 1:259–260
Defense Information Systems Agency, U.S (DISA), **1:320**
Defense Intelligence Agency, United States
sections and directorates, 1:328–329
Defense Intelligence Agency, United States (DIA), **1:327–329**
remote viewing experiments, 2:452
Defense Meteorological Satellite Program (DMSP), 2:340–341
Defense Nuclear Facilities Safety Board (DNFSB), U.S., **1:321**
Defense Security Service, U.S., **1:321–322**
Defense Support Program satellites (DSP), 3:47–49
De Lome letter forgery, 1:344
Delta Force, **1:322–323**
Democratic National Committee
Chinese contributions to, 1:190–191
Department of Defense (DOD), 1:252, **1:350–353**
bio-flip implant research, 1:112
BMDO, 1:86
Chemical and Biological Defense Information Analysis (CBIAC), 1:174
Defense Information Systems Agency, U.S (DISA), 1:320
dual use technology, 1:364–365
history of, 1:350–351
intelligence agencies in, 3:204
leadership and commands, 1:352–353
NASA joint programs with, 2:298–299
resources of, 1:351–352
Department of Energy (DOE), 1:53, **1:353–356**
Atmospheric Release Advisory Capability (ARAC), 1:68–69
comprehensive energy plan, 1:354
Department of Energy Organization Act (1977), 1:354
Nuclear facilities safety board, 1:321
programs and offices, 1:354–356
Department of Health and Human Services (U.S.)
bioterrorism initiative, 1:126
Department of Homeland Security, 3:71
Operation Liberty Shield, 2:385–386
Desch, Joe, 1:*137*
De Souza, Steven E. (screenwriter), 1:259–260
DEST. *See* Domestic Emergency Support Team (DEST)
Detection technologies
biotechnology programs, 1:110–111, 1:119
bombs, 1:135–*136*
chemical and biological, 1:175–176, 3:260–263
Los Alamos National Laboratory, 2:239–241
metal detectors, 2:254–256
nuclear, 2:240, 3:260–262
PNNL research in, 2:395
polymerase chain reaction (PCR), 1:117, 2:56, 2:379, 2:433–436
radiation detector, 1:144
sensor development, 1:143
sniffer dogs, 1:163–165
solid-phase micro extraction techniques, **3:89**
X-ray machines, 1:175
Deutch, John M., 1:196, 1:311
Deuterium, 2:81–82, 2:247
Dewey, George, 3:102–103
Dexamphetamine "go" pills, 1:270
Dial tone decoder, **1:329**
Digital Encryption Standard, 1:227
Digital Globe, 3:44
Digital Millennium Copyright Act (DMCA), 1:272
Digital photography, 2:422–423
cameras, 2:423
charged coupling devices (CCD), 2:422
encrypted watermarking, 2:423
See also Cameras; Photography
Digital signatures, 1:262, 2:446
Directed energy weapons
Radio frequency (RF) weapons, 3:5–6
space-based, 3:122
Directorate of Science and Technology (DS&T, CIA), **1:197–198,** 1:201
psychic "remote viewing" of sites, 1:198
Director of Central Intelligence (DCI), **1:308–312**, 2:444–445, 3:203–204
Dirty tricks, **1:331**
Egyptian embassy cipher room bugged, 1:404–405
DISA. *See* Defense Information Systems Agency, U.S (DISA)
Disaster relief
Disaster Relief Act (1974), 2:15

How to go to your page

See also Federal Emergency Management Agency (FEMA)
Disinformation campaigns, **1:331–324,** 2:450
DNA detection and identification
biological weapons, 1:342
DNA signatures, 1:342
Human Genome Project, 2:265
of humans, 1:337, 1:341, 2:36–37, 2:*37*
hybridization assays, 1:*339,* 1:339–340
polymerase chain reaction (PCR), 1:117, 2:56, 2:379, 2:433–436
recognition instruments, **1:338–340**
DNA fingerprinting, **1:336–338**
genetic disease detection, 2:54
process of, 1:337–338
DNA genome
structure of, 1:341
unique sequences, **1:340–342**
DNA microarray technology, 2:56
DNA science and technology, **1:335–336**
analysis aided by biosensor technology, 1:112
bacterial DNA, 1:80–81
biodetectors, 1:110–111
databases for identification, 1:73, 1:85
electrophoresis separation, 1:391
encoding secret messages, 1:341–342, 2:265, 2:279
implants into biological systems, 1:114–115
nanotechnology applications in, 2:295
profiling, 1:185
radiation damage to, 3:3
recombinant, 2:56, 2:406–407
sequences, **1:340–342**
viral genetics, 3:237–239
Watson-Crick model, 1:335
DNFSB. *See* Defense Nuclear Facilities Safety Board (DNFSB), U.S.
Document destruction, **1:342–344,** 1:*343*
burn box, 1:343
Document forgery, **1:344–350**
Document security
shredding, 1:343
DOE. *See* Department of Energy (DOE)
Doe, Sgt. Samuel K., 1:8
Dogs
search and rescue at WTC, 2:*15*
sniffer, 1:164–165
Dolphins (Marine Mammal Program), 2:249–251, 2:*250*
Domestic Emergency Support Team (DEST), **1:356–357**
Domestic intelligence, **1:357–358**
Domestic Preparedness Office, U.S. National (NDPO), **1:358**
Domestic terrorist groups, 3:142–144
Dominican Republic, U.S. intervention in, 1:29
Donovan, William J., 1:199–200, 2:390, 3:208
Doo transmitter, **1:359**
Dosimeters, 1:359–360
Dosimetry, **1:359–360**
Double agents, **1:360–361,** 2:203
Aldrich H. Ames, 1:31–33
Aleksander Ogorodnik, 1:298
counterintelligence and, 1:275
George Blake, 1:102
Robert Philip Hansen, 1:316, 2:77–78
Downey, John T., 2:*207*
Doyle, Arthur Conan (1859–1930), 2:131
forensic geology usage in *A Study in Scarlet,* 2:33
Drug Control Policy, U.S. Office of National, **1:362**
Drug Enforcement Administration, U.S. (DEA), **1:312–315,** 1:*313*
interaction with FBI, 1:314
programs and goals, 1:315
Drug-Free Communities Act (1997), 1:362
Drugs and narcotics
barbiturates use as "truth serum," 3:173
canine substance detection, 1:163–165
International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139–140
socially acceptable during 1970's, 1:313
Drug trafficking
Bolivia, 1:133
narco-terrorism and, 1:281, 1:314
Drug war, 1:30–31
anti-drug advertising, 1:362
DEA intelligence on, 1:314
Department of Defense lead agency for, 1:147
Reagan administration and, 1:313
Special Anti-narcotics Force (Bolivia), 1:133
Drug war intelligence
National Drug Intelligence Estimate (NDIE), 1:363
NORAD tracking, 2:345
DS&T. *See* Directorate of Science and Technology (DS&T, CIA)
Dual use technology, **1:364–365**
Duarte, Jose Napoleon, 1:29, 1:30
Ducket, Carl, 2:452
Dudayev, Pres. Dzhozkhar (Chechnya), 1:172–173
Dulles, Alan W., 1:195, 1:309–310
as Secretary of State, 1:325
Secret Intelligence Branch, 2:390
Dzhoney, Nikolay Volodiev, 1:*220*

E

E-2C Hawkeye aircraft, **1:367–368**, 1:*367*
Eastern Europe, Soviet communism in, 1:230–231
East German intelligence agency (STASI), **3:114–115,** 3:*115*
Ebola virus, **1:368–369**
E-bombs, **1:369–370,** 1:384
Echelon surveillance system, **1:370–372**
communication intercepts, 1:386
privacy rights and, 2:448
Echosounders
use in bathymetric mapping, 1:95
Economic espionage, **1:372–374**
Economic Espionage Act (1996), 1:*190,* 1:372, 1:374
MI6 and, 2:262
U.S. industry effects of, 1:373
vulnerabilities of, 1:372–373
Economic intelligence, **1:374–376**
foreign, 1:375
Office of Research Reports (ORR), 1:374
resources, 1:375–376
Economic interests and controls
for Chad oil revenues, 1:9
Marshall Plan (1947), 1:232, 1:233
Soviet Molotov Plan, 1:232
Economy, U.S.
maintaining stability, 2:13–14
open market operations, 2:13
Edmonds, Emma, 1:*210,* 1:212
Egypt
espionage in ancient, 1:416
intelligence and security, **1:376**
London embassy bugged during Suez crisis, 1:404–405
looting of historical artifacts, 1:46
Egyptian Islamic Jihad, 1:25
Al-Qaeda and the World Islamic Front for Jihad, 1:26
Eichmann, Adolf, **1:376–378,** 1:*377*
Einstein, Albert, 1:399, 2:22, 2:246, 2:295, 2:374
Eisenhower administration (1953–1961)
China and Korean War, 1:379
Cuba intervention, 1:29
Eisenhower Doctrine, 1:237
end of Korean war, 2:208–209
Middle East independence of nations doctrine, 2:273
National Security Council, 2:356
national security policy, **1:378–379**
New Look program, 1:235
plan to depose Fidel Castro, 1:96
Project GENETRIX, 1:93–94
Sen. McCarthy and, 1:235
Southeast Asian Treaty Organization (SEATO), 1:237, 1:379
Tachen Straits crisis and nuclear threat, 1:237
Eisenhower-Rockefeller letter forgery, 1:347
El Salvador, 1:29

civil war in, 1:30
intelligence and security, **1:379–380**
Electromagnetic spectrum, **1:381–384,** 1:388–389
imaging technology, 1:392–393
military and security significance of, 1:383–384
multi and hyperspectral imagery, 2:60
Electromagnetic weapons
biochemical effects, **1:384–385**
electromagnetic pulse (EMP), **1:380–381**
Electronic communication intercepts
Echelon, 1:370–372
legal issues, **1:385–387**
Electronic Communication Privacy Act (1986), 1:146
computer crimes, 1:256
Electronic Communications Privacy Act (1994), 2:146
Electronic countermeasures, **1:387–388**
Electronic data destruction, **1:255**
Electronic devices
limits of conventional, 2:461
screening for, 1:22
Electronic intelligence (ELINT)
by aerial reconnaissance, 1:75
Echelon, 1:370–372
HUMINT *vs.,* 1:385
P-3 Orion aircraft modified for, 2:393
ships designed for, 3:76–77
TEMPEST technology, 1:385
Electronic locks and keys, 2:236
Electronics intelligence (ELINT)
Electronic voice alteration, **3:242**
Electronic warfare, **1:388–390**
countermeasures to, 1:387–388
e-bombs, 1:389–390
electromagnetic pulse, 1:369–370
Electron microscopy, 2:271
Electro-optical intelligence, **1:390**
Electrophoresis, **1:391–392**
ELINT. *See* Electronic intelligence (ELINT)
Ely, Eugene, 1:19
Emergency planning
Continuity of Government program (COG), 1:269–270
Crisis Relocation Facilities, 1:269
DOE Emergency Operations office, 1:355
emergency response drill, 1:*354*
EPA training and environment monitoring, 1:411
military-civil training center, 2:303–304
National Response System, 1:394
Radiological Emergency Response Plan, 3:8
Emergency Planning and Community Right-to-Know Act (EPCRA), 1:178, 3:200
Emergency Response Teams, **1:393–395,** 1:*394*
Emergency Response Technology Program (ERT), 3:136–137
Emergency services
Domestic Emergency Support Team (DEST), 1:356–357
EM wave scanners, **1:392–393**
Encryption standards
Advanced Encryption Standard, 1:227, 1:228, 1:291, 1:396
Data Encryption Standard, 1:207, 1:289, 1:291, 1:396
Digital Encryption Standard, 1:227
Escrowed Encryption Standard (EES), 1:218
GSM mobile phone, 2:73–74
Encryption systems and devices, 1:131–133, 1:286, 1:319–320
algorithms, 1:396, 2:73
of data, **1:395–396**
Energy Department (DOE), United States. *See* Department of Energy (DOE)
Energy directed weapons, **1:399–400**
Energy harvesting, 3:26–27
Energy policy
energy crisis (1973–1974), 2:384
energy technologies, **1:401–403**
OPEC, 2:315, 2:384–385
security issues, 1:402, 2:314–315
Energy Regulatory Commission, U.S. Federal (FERC), **1:401**
Energy Reorganization Act (1974), 1:354, 2:370
Engelmann, Rudy J., 1:68
Engineered Tissue Constructs (ETC), **1:111–112**
Engines, scramjet, 2:91–92
Engraving and Printing, U.S. Bureau (BEP), **1:403–404**
ENIAC machine, 1:243
Enigma cipher machine (WW II Germany), 1:131–132, 1:205, 1:*206,* 1:291, **1:405–407,** 1:*406*
bombe development for deciphering, 1:131, 1:137, 1:206
scrambler, 1:406–407
U.K.—U.S. sharing of information on, 3:106
Enterprise (aircraft carrier), 1:19
Entertainment industry, simulations for defense industry, 1:259–260
Entry-Exit Registration System, U.S. National Security, **1:408**
Environmental Measurements Laboratory, **1:409–410**
Environmental policy
Environmental issues impact on security, **1:408–409**
EPA programs, **1:410–411**
national security effects on, 1:409
EPA (Environmental Protection Agency)
Emergency Response Teams, 1:393–395
National Response Team, 2:306–307
EPCRA. *See* Emergency Planning and Community Right-to-Know Act (EPCRA)
Epidemiological Intelligence Service, 1:168
Epidemiology, **1:411–413**
ERT. *See* Emergency Response Technology Program (ERT)
Espionage, **1:413–414**
Cambridge University Spy Ring, 1:151–155
Chinese in U.S., 1:190–191, 2:133
computer keystroke recorder, 1:258–259
corporate, 1:255–256
covert operations, 1:276–279
Cuban operations against U.S., 1:292–293, 1:*414*
early U.S., 3:22
economic, 1:*190,* 1:342, 1:372–374
in the Middle Ages, 1:417–418
surveillance cameras in, 1:156–157
Espionage Act (1917), **1:415**
Socialist Party (U.S.), 2:122
Espionage and intelligence
historical foundations, **1:415–420**
Soviet and Russian moles, 2:280–281
Espionage technology and tools
cameras and microfilm, 2:267–268
drops, **1:361**
impact of industrialization, 1:419
KGB, 2:202–203
tradecraft, 3:167
World War I, 1:2
Estonia, intelligence and security, **1:420**
ETA. *See* Basque Fatherland and Liberty (ETA)
Ethiopia, 1:7–8
Ethnic profiling
in screening process, 1:22
Euckadi Ta Askatasuna. *See* Basque Fatherland and Liberty (ETA)
European colonies (African), 1:6
European Union, **1:420–422**
European Union agencies, 1:422
Evers, Medger, 2:8
Executive orders and Presidential directives, **1:422–423,** 2:309
Expendable launch vehicles, 2:298–299
Explosive coal, **1:423–424**
Explosives Unit (FBI)
bomb damage assessment, 1:134
Extraterrestrial Highway, 1:*52*
Extraterrestrial life and UFO's, 1:51

F

F-22 Raptor, 1:*388*
F-117A Stealth Fighter, **2:1,** 2:*2,* 3:*116*
F/A-18 Hornet, 1:*18,* 1:*400*

FAA (Federal Aviation Administration, U. S.), **2:2–3**
data parameter requirements for FDRs, 2:26
emergency responses to 9/11, 3:70
Facility security, **2:4–5**
Fair Credit Reporting Act (FCRA), 2:448
Fair Employment Practices Commission (FEPC), 2:7
Fatah Revolutionary Council. *See* Abu Nidal Organization (ANO)
FATF. *See* Financial Action Task Force (FATF)
Faulds, Henry (fingerprint identification), 2:17
FBI Explosives Unit
bomb damage assessment, 1:134
FBI (Federal Bureau of Investigation, U. S.), 1:13, **2:5–9**
assistance following chemical attacks, 1:179
COINTELPRO operations, 1:229–230, 2:8
computer keystroke recorder, 1:258–259
forensic use of DNA, 2:9
interaction with DEA, 1:314
PENTTBOM (9/11) investigation, 3:71
response to spy ring defections, 1:154
Un-American Activities Committee, U.S. House (HUAC), 2:253
United States v. Scarfo, 1:258–259
FBI (Federal Bureau of Investigation, U. S.) administration
careers in, 2:120–121
computer systems security measures, 2:8
counter-terrorism focus, 2:220–221
Freedom of Information Act requirements, 2:27, 2:28
history of, 2:6–8
FCC (U.S. Federal Communications Commission), **2:9–10**
FM transmitter regulations, 2:26–27
National Telecommunications Information Administration, U.S. (NTIA), 2:312
radio frequency regulations, 3:5
FCRA. *See* Fair Credit Reporting Act (FCRA)
FDA (U.S. Food and Drug Administration), **2:10–11**
branch of HHS, 2:81
Public Health Service and, 2:455
Federal air marshals (FAM), 1:14–16, 1:*15*
Federal Aviation Act (1958), 2:2
Federal Emergency Management Agency (FEMA), **2:14–16**
assistance following chemical attacks, 1:179
Coast Guard National Response Center, 1:223
Crisis Relocation Facilities, 1:269
Mount Weather, 2:285–286
Radiological Emergency Response Plan, 3:8
World Trade Center activities, 1:50, 2:*15*
Federal Firearms Act (1938), 1:68
Federal language schools and tests, 2:216
Federal Open Market Committee, 2:*13,* 2:14
Federal Property and Administrative Services Act (1949), 2:11, 2:51
Federal Protective Service, U.S., **2:11–12**
Federal Railroad Administration (FRA)
Coast Guard National Response Center, 1:223
Federal Republic of Germany (FRG), 1:103
Federal Reserve Act (1913), 2:12
Federal Reserve System, U.S., **2:12–14**
banks in, 2:14
Federal Wiretapping Act (1968), 2:448, 3:138
FEMA. *See* Federal Emergency Management Agency (FEMA)
FEPC. *See* Fair Employment Practices Commission (FEPC)
FERC. *See* Energy Regulatory Commission, U.S. Federal (FERC)
Fermi, Enrico, 2:23, 2:247
FEST. *See* Foreign Emergency Support Team, U.S. (FEST)
Fe Ye, 1:373
Feynman, Richard, 2:246
Fibonacci, Leonardo (13th century mathematician), 1:288
Fighting Islamic Group, 1:25
Financial Action Task Force (FATF), 3:155, 3:157, 3:158
Financial intelligence
counterintelligence efforts, 1:73
Fincher, David (film director), 1:259
Fingerprinting analysis, **2:17–19**
Fingerprinting identification systems, 2:*18,* 2:19, 2:95
Finland, intelligence and security, **2:19–20**
First of October Anti-Facist Resistance Group (GRAPO), **2:20**
FISH (Geheimschrieber cipher machine). *See* Geheimschrieber cipher machine (WWII Germany)
Fission. *See* Nuclear fission
Flame analysis, **2:24–25**
Fleischmann, Martin, 2:45
Fleming, Ian, 2:132
Bond movies, 2:287–288
Flight crews (aircraft carriers), 1:18
Flight data acquisition unit (FDAU), 2:26
Flight data recorders, 2:*25,* **2:25–26**
data parameters recorded, 2:26
Flowers, Tommy, 1:242, 3:184
FM transmitters, **2:26–27**
FOIA. *See* Freedom of Information Act (FOIA,1967)
Food supplies
Food and Cosmetic Act (1938), 2:10
Food and Drugs Act (1906), 2:10
Food contamination, 3:310
protection from bioterrorism, 2:29
Ford administration (1974–1977)
CIA restrictions, 1:194, 1:203
loss of S. Vietnam to communists, 2:30
National Security Council, 2:357
national security policy, **2:30**
Foreign Assets Control, U.S. Office (OFAC), **2:31**
Foreign Broadcast Information Service (FBIS), **1:198–199**
Foreign economic intelligence, 1:375
Foreign Emergency Support Team, U.S. (FEST), **2:16–17**
Foreign Funds Control (1940), 3:171
Foreign Intelligence Advisory Board, 1:194, 1:203
Foreign Intelligence Surveillance Act, **2:31–32,** 2:133, 2:448
Foreign Intelligence Surveillance Court of Review, **2:32–33**
Foreign technology intelligence
assisted strategic arms treaties, 1:76
U.S. economic espionage in, 1:373
Forensic chemistry, 1:183
chemical traces, 2:37
DNA fingerprinting, 1:338
solid-phase micro extraction techniques, 3:89
Forensic geology
in criminal investigations, 2:34–35
in military or intelligence operations, **2:33–35**
Forensic science, **2:36–39**
analytical methods, 2:38–39
bomb damage, 1:134
chemical applications in, 1:183–185
DNA fingerprinting in, 1:337
evidence and examination, 2:36–38
FBI's use of, 2:6–7
geology, 2:33–35
nuclear magnetic resonance, 2:373
nuclear spectroscopy, 2:372–373
polymerase chain reaction (PCR), 1:117, 2:38, 2:56, 2:433–436
seismology, 2:35
toxicology, 3:165
Forensic voice and tape analysis, **2:39–40**
Forrestal (aircraft carrier), 1:19
Fouché, Joseph, 2:296–297
FRA. *See* Federal Railroad Administration (FRA)
France
aircraft carrier development, 1:19–20
balloon flight development, 1:91–92, 1:93
counter-terrorism policy, **2:40–41**
espionage in 19th century Great Britain, 2:297–298
French underground during World War II, 2:42–43
intelligence and security, **2:41–42**

U.S.—Iraq anti-war position, 2:165
withdrawal from Vietnam, 3:232
Franco-Prussian War, 1:2
Franklin, Benjamin, 1:91
first postmaster general, 2:442
Franks, Tommy R., 2:170
Freedom of Information Act (FOIA,1967), **2:27–28**
Freedom of Information-Privacy Acts (FOIPA), 2:28, 2:447–448
French underground (World War II)
communications and codes, **2:42–43**
Jedburghs working with, 2:390
Friedman, William, 2:460
Fuel cells
research in hydrogen, 1:354, 1:402
Fulbright, J. William, 2:189
Fusion. *See* Nuclear fusion

G

G-2, **2:47**
Galton, Sir Francis (fingerprint identification), 2:17
Gamma rays
role in EMP weapons, 1:383
Gamow, George, 2:52
GAO (General Accounting Office, U.S.), **2:48**
Gas chromatography-Mass spectrometer, 1:175, 2:38–39, **2:49–50,** 2:*50*
Gates, Robert, 1:*148,* 1:196, 1:311
Clinton intelligence briefing, 2:429
Gaulle, Charles de, 2:43
French involvement in Vietnam, 3:232
Geheimschrieber cipher machine (WWII Germany), 1:205–206, **2:21**
Geller, Uri (psychic), 2:453
General Services Administration, U.S. (GSA), **2:51**
Genetic code, **2:52–54,** 2:*53*
Genetic engineering
DNA implants, 1:114–115
identifying and detecting biological weapons, 1:118, 2:278–279
recombinant DNA, 2:278
of vaccines, 3:86
See also DNA science and technology
Genetics
Austrian database for identification, 1:73
bacterial, 1:82–84
disease detection and treatment, 2:54, 2:57
epidemiology, 1:412
ethics, privacy and security issues, **2:54–55**
technology of, **2:56–57**
testing, 2:*53,* 2:55
viral, 3:237–239
See also DNA detection and identification; DNA science and technology
Geneva conventions, 2:124–125
Geneva Protocol (1925)
diplomatic control of biological weapons, 1:116
Genomics, **2:57–58**
applications of, 2:57–58
sequencing of pathogens, 2:404
of viruses, 3:237–238
Geographic Information Systems (GIS), **2:64–65,** 2:248
crisis management and, 2:221–222
LIDAR system and, 2:234–235
Geological Survey, U.S. (USGS), 2:425
Geology
forensic, 2:33–35
military use of terrain intelligence, **2:58–59**
radar mapping and remote sensing, 2:59
Geospatial imagery, **2:59–60**
German-Bolshevik conspiracy forgery, 1:345–346
German Democratic Republic (GDR), 1:103
Germany
aerial reconnaissance, 1:74
Berlin Wall divides country, 1:103
counter-terrorism policy, **2:61**
cryptography, 1:3–4, 1:131–132, 1:291
East Berlin borders closed, 1:105–106
intelligence agencies, 1:2–3
intelligence and security, **2:62–63**
V-2 missile, 1:87, 1:89
WWI sabotage and intelligence operations, 1:129–130
See also Nazi Germany
Gestapo, 1:3, **2:63–64**
Ghauri (Pakistan), 1:*88*
GIA. *See* Armed Islamic Group (GIA)
Gibson, Steve, 1:*262*
Gibson, William, 1:264
GIS (Geographic Information Systems), **2:64–65,** 2:248
crisis management and, 2:221–222
LIDAR system and, 2:234–235
Giuliani, Rudolph, 1:314
Global Communications, U.S. Office (OGC), **2:66**
Global Expertise Reserve Program (GERP), 2:326
Global Positioning System (GPS). *See* GPS
Global Protection Against Limited Strikes (GPALS), 3:124
Global Seismograph Network, 3:64
Glomar Explorer, **2:66–67**
Goldwater-Nichols Department of Defense Reorganization Act (1986), 2:190
Goleniewski, Michael, 2:281
Gorbachev, Mikhail (Soviet Premier), 2:202
announces nuclear testing moratorium, 1:254
Glasnost or "openness" and anti-Communist movements, 1:241
Soviet economy and reforms, 1:240–241
Göring, Herman, 2:63
Gorshkov (aircraft carrier), 1:20
Gottlieb, Sidney (1918-), 1:108
Government buildings
Federal Protective Service security of, 2:11–12
GSA approved designs, 1:50, 2:51
Oklahoma City Federal Campus, 1:49
Ronald Reagan building, 1:49
security of, 1:50, 2:136–137
Government Ethics, U.S. Office (OGE), **2:68**
Government information
classification procedures, 1:213
Classified National Security Information Act, 1:214–215
Freedom of Information Act, 2:27–28
See also Classified information
Government officials
protection of, 1:269–270
Shadow Cabinet, 1:269
GPS (Global Positioning System), **2:68–70,** 2:*69,* 2:*70*
LIDAR system and, 2:234–235
mapping accuracy, 2:248
GRAPO. *See* First of October Anti-facist Resistance Group (GRAPO)
Graves, Harold N. (FBIS director), 1:198
Great Depression, crime rates, 2:6
Great Game, **2:70–72**
Great Game Anglo-Russian Convention (St. Petersburg, 1907), 2:72
Greece
espionage in ancient, 1:416
intelligence and security, **2:73**
repatriation of Elgin Marbles, 1:46
Soviet incursions in, 1:233
Greenspan, Alan (Federal Reserve chairman), 2:13
Grenada
Operation Urgent Fury, 1:29
U.S. invasion of, 3:*10*
Groves, Brig. Gen. Leslie, 2:*246*
Gruinard Island, 3:*109*
GSA, 1:49
government building approved designs, 1:50
GSM Encryption, **2:73–74**
Guatemala, intelligence and security, **2:74**
Guerilla warfare, **2:74–75**
Gun control legislation, 2:195
Federal Firearms Act (1938), 1:68
Gun Control Act (1968), 1:68
National Firearms Act (1934), 1:68

Organized Crime Act (1970), 1:68
Guns
ballistic fingerprints of, **1:85**
concealment techniques, 1:65
plastic bullets, 2:*231*
poison firing devices, 1:63–64, 1:65
residue analysis of, 1:184
revolvers, 1:*63*
silencers, **3:80–82**
submachine, 1:*59*
Taser, 3:134–135
Guzman, Abimael, 1:31

H

Habash, George, 2:436
Habeas Corpus Act (1863), 2:121–122
Habyarimana, Maj. Gen. Juvenal, 1:7
Hackers. *See* Computer hackers
Hagalin, Boris (Swedish inventor), 1:206
Hager, Nicky, 1:372
Hague conferences, 2:124–125
Hahn, Otto (scientist, 1859–1968), 2:22, 2:375
Haig, Alexander, 2:358, 3:9
Haiti
intervention in, 1:30
Hale, Nathan, 1:*417,* 3:*21*
Hall, Reginald, 3:28
Halverson, Lt. Gail, 1:100
HAMAS (Islamic Resistance Movement), **2:77**
Hamilton, Alexander, 1:66, 3:169
Hansen, Robert, espionage case, 1:316, 1:361, **2:77–78,** 2:280–281
Harakat ul-Jihad Islami/ Bangladesh (HUJI-B) (Movement of Islamic Holy War), **2:79**
Harakat ul-Jihad Islami (HUJI) (Movement of Islamic Holy War), **2:78–79**
Harakat ul-Mujahidin (HUM) (Movement Holy Warriors), **2:79–80**
Hardening (computer systems), **2:80**
Harrier Jet, 1:20
Hassan-i-Sabah, Ismaili (1090 AD), 1:60
Hastart, U.S. Rep. Dennis, 1:*214*
Havel, Czech Pres. Vaclav, 1:*303*
Hayden, Michael, 2:*352*
Hazardous waste disposal
byproducts and waste, 2:369–370, 2:371, 2:381
PNNL research in, 2:394
Sandia Lab research in, 3:38
Health and Human Services Dep't, U.S., **2:81**
Healthcare Research and Quality, Agency for (AHRQ), 2:455
Health Resources and Services Administration (HRSA), 2:455
Heavy water technology for nuclear development, **2:81–83,** 2:82–83, 2:247
Hebern, Edward, 1:291
Hegel, Georg W.F. (1771–1830), 3:148
Heinzen, Karl (1809–1880), 3:150
Heisenberg, Werner, 2:295
Helgerson, John L.
Clinton intelligence briefing, 2:429
Hellings, Martin, 3:102
Helms, Richard McGarrah, 1:196, 1:310
Helvey, Ephraim, 2:*283*
Hemlock
as a biochemical weapon, 1:106
Hemorrhagic fevers and diseases, **2:83–84**
Henry, Sir Edward (fingerprint classification), 2:17
Herzegovina. *See* Bosnia and Herzegovina
Heydrich, Reinhard, 1:2, 2:63
Hezbollah, 2:204
High-altitude Electromagnetic pulse (HEMP), 1:380–381
High power microwave weaponry, 1:399, **2:271–272**
Hillenkoetter, Rear Admiral Roscoe H, 1:195, 1:309
Himmler, Heinrich, 1:3, 2:63, 2:*64*
Hindenburg airship crash, 1:93
Hinkley, Jr., John
gun used in assassination attempt, 1:*63*
Hiroshima, Japan, 1:231, 2:23, 2:246
Hiss, Alger, 2:252
Hitchcock, Alfred (spy movies), 2:286
Hitler, Adolph (1889–1945), 2:63, 3:276, 3:278
Hizballa (Party of God), **2:84–85**
Ho Chi Minh (N. Vietnam leader), 3:232
Hollywood blacklist, 2:*252*
Holocaust
first intelligence on, 1:133
"Great Theft" of artwork, 1:47
Homeland Security, U.S. Dept. of, **2:85–88**
airline security, 1:22, 1:44–45
framework and directorates of, 2:87–88
Tom Ridge and, 1:*124,* 2:*86*
U.S. Coast Guard, 1:221, 2:87
Homeland Security Act, 2:86
Homeland Security Advisory System (HSAS), 3:140–142
Homing devices
doo transmitter, 1:359
Honecker, Ulbrecht Erich (Berlin Wall builder), 1:105
Hooke, Robert, 2:270
Hoover, J. Edgar (FBI director), 2:6
Un-American Activities Committee, U.S. House (HUAC), 2:253
Horsley, J. Stephen, 3:173
Houseman, John, 3:244
HUAC. *See* Un-American Activities Committee, U.S. House (HUAC)
Huang, John, 1:190
Hubble Space Telescope, 3:97
Hughes, Howard, 2:66–67
Hughes Electronic Corporation
Chinese rocket information exchange, 3:42
Hughes-Ryan Act (1974), 2.135
Human air plume, 1:16–17
Human decontamination, 1:316, 1:318–19
Human Genome Project, 2:55
microorganism detection and identification, 2:265
HUMINT (Human Intelligence), 1:193, **2:89**
ELINT *vs.,* 1:385
used during Spanish-American War, 3:102–103
Hungary, intelligence and security, **2:90**
Hussein, Saddam, 2:162, 2:414–416
assassination attempt on Bush (H.W.), 2:416
48-hour deadline, 2:166
regime toppled, 2:175–176
war against, 2:169–176
See also Iraq; Operation Iraqi Freedom
Hwei Chen Yang, 1:*190*
Hydrogen bomb, 2:375, 3:258
Truman asks for, 1:232
Hydrogen fuel cell research, 1:354, 1:402
HyperSoar hypersonic aircraft, 2:91
Hypersonic aircraft, **2:90–92**
Hyperspectral imagery, 2:60, 2:248

I

IBIA. *See* International Biometric Industry Association (IBIA)
IBIS (Interagency Border Inspection System), 1:45, **2:93–94,** 3:72
IDENT (Automated Biometric Identification System), **2:95**
Identification Friend or Foe (IFF), **2:98**
Identification systems
Automated Biometric Identification System (IDENT), 2:95
Identity theft, 1:342, **2:96–97**
Identity theft affidavit, 2:97
Identity Theft and Assumption Deterrence Act (1998), 2:97
Identity Theft Data Clearinghouse, 2:97
Pickler, Nedra (reporter), 2:*96*
IFF (Identification Friend or Foe), **2:98**
IKONOS remote sensing satellite, 3:43
Image intensification, 2:327–328
Image processing
electromagnetic spectrum, 2:248
software, 3:13–14
Imagery intelligence, 1:11–13, 1:*12,* 1:193, **2:99–100**
IMF (International Monetary Fund), **2:98–99**
Immigration and Naturalization Services (INS), **2:113–114**

Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS), **2:115–116,** 2:439
IMS. *See* International Monitoring System (IMS)
India
aircraft carrier development, 1:19
intelligence and security, **2:100–101**
looting of historical artifacts, 1:46
Indian Health Services (IHS), 2:455
Indonesia, intelligence and security, **2:101–102**
Industrial Security Program (ISP), 1:321–322
Infectious diseases, 1:170
epidemiology tracking, 1:411–413
Federal quarantine legislation, 1:250
hemorrhagic viruses, 2:83–84
pathogen transmission, 2:404–405
SARS isolation and quarantine, 1:248–252
security threats, **2:102–105**, 2:*103,* 2:264–265
smallpox, 3:84–85
underdeveloped countries susceptible to, 2:104
zoonoses, 3:286–287
Information security, **2:105–106**
anti-virus software and, 2:105
breaches of, 2:105
cryptography and, 2:105–106
Information Security, U.S. Office (OIS), 2:106
Information Security, U.S. Office (OIS), **2:106**
Information Sharing and Analysis Centers (ISACs), 1:301
Information warfare, **2:107–110**
Infrared detection devices, 2:110, **2:110–112**
cameras, 1:390, 2:111
military applications for, 2:111
motion sensors, 2:284–285
police and security applications, 2:111–112
Infrared imagers
countermeasures for, 2:112
designs for, 2:111
Infrared spectroscopy, 3:107
Infra-red waves
night vision and, 1:382, 2:111
stealth technologies, 3:117
Infrastructure
components of, 1:282
Critical infrastructure Assurance Office (CIAO), 1:282–283
Infrastructure Protection Center, U.S. National (NIPC), 2:112–113
protection of, 1:283, 3:62
Infrastructure Protection Center, U.S. National (NIPC), **2:112–113**
Inman, Admiral Bobby R., 1:330
INS (Immigration and Naturalization Services), **2:113–114**
InSAR (Interferometric Synthetic Aperture Radar), 2:248, 3:14
INSCOM (U.S. Army Intelligence and Security Command), **2:114–115**
Insecticide research, 2:321–322
INSPASS. *See* Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS)
Inspector General, Office of the (OIG), **2:116–117**
Institute for Creative Technologies, 1:260
Institute of Future Space Transport, 2:*91*
Insurance industry, terrorism risk insurance, **3:151**
Intelligence, **2:117**
briefings to presidential candidates, 2:429
careers in, 2:119–121
history of U.S., 3:206–209
Intelligence agencies
aiding crime prevention, 1:280–281
early U.S., 3:21
Intelligence agent, **2:117–118**
International law and, 2:125
types of agents, 2:118
Intelligence and counter-espionage careers, **2:119–121**
Intelligence and democracy
anti-communism hysteria, 2:122–123
civil rights and liberties, 2:121–122
COINTELPRO illegal operations discrediting groups, 1:229–230
individual privacy and investigation policy, 2:123–124
issues and conflicts, **2:121–124**
Patriot Act and, 1:386–387
Intelligence and international law, **2:124–125**
Intelligence and Research, U.S. Bureau of (INR), **2:127**
Intelligence and Security Committee, U.K., 2:168
Intelligence and Threat Analysis (ITA), 1:330
Intelligence Authorization Acts, U.S. Congress, **2:128**
Intelligence community, **2:128–130**
American and European communities (WW I), 3:270–271
changes during Spanish-American War, 3:103
defining and formation of, 2:128–129, 3:21–22
Intelligence Community Executive Committee (IC/EXCOM), 2:129–130
Joint House-Senate Intelligence Committee, 2:*129*
oversight of, 1:194, 2:130, 2:135–136
psychotropic drugs and, 2:454–455
reorganization under National Security Act, 2:307–308
restrictions on, 2:126
tradecraft, 3:167
United States, 3:202–204
U.S. President and, 2:444–445
Intelligence Identities Protection Act (1982), 1:203
Intelligence Information Act (annual), 2.136
Intelligence literature, **2:130–132**
Intelligence officer, **2:133**
Intelligence Oversight Act (1980), 1:203
Intelligence Policy and Review, U.S. Office of (OPIR), **2:133–134**
Intelligence research
Bureau of Intelligence and Research (INR) U.S. State Dep't, 1:323–324
Intelligence and Threat Analysis (ITA), 1:330
National Intelligence Estimates (NIEs), 1:324
Office of Research Reports (ORR, CIA), 1:374
Intelligence retrieval
dead drop spike, 1:315
dead letter box, 1:315–316
ships designed for collection and, 3:76–77
Intelligence Services Act, U.K. (1994), 2:262
Intelligence sources, 1:193, 1:199
in Civil War escaped slaves as, 1:211
computer keystroke recorder, 1:258–259
data mining and databases, 1:307–308
dumpster diving, 1:299–300, 1:342
Intelligence Support, U.S. Office of, **2:134**
Interagency Border Inspection System (IBIS), 1:45, **2:93–94,** 3:72
Interagency Security Committee, U.S., **2:136–137**
Intercontinental ballistic missiles (ICBMs), 2:*374,* 3:*261*
Minuteman ICBM (U.S.), 1:*87,* 1:90
NORAD tracking, 2:345
See also Ballistic Missiles
Internal Revenue Service (IRS), 1:68, **2:137–138**
Criminal Investigation division, 2:138
Restructuring and Reform Act (1998), 2:137
International Atomic Energy Agency (IAEA), **2:138–139**
Chernobyl disaster efforts of, 2:139
Iranian nuclear programs, 2:160–161, 2:164
LANL programs used by, 2:240
limitations of, 2:138–139
North Korea restricting inspections of, 2:347–349
nuclear weapon trafficking reports, 3:32
tracking nuclear materials, 3:255–257
International Biometric Industry Association (IBIA), 1:121

International Border Interdiction Training, 1:*297*
International Commission on Missing Persons, 2:*37*
International crime
International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139
International Fusion Program, 2:45–46
International law
blocking terrorist financing, 3:158–159
Geneva conventions, 2:124–125
Hague conferences, 2:125
intelligence and, 2:124–125
International Law Enforcement Academies (ILEAs), 2:139
International Monetary Fund (IMF), **2:98–99**
International Monitoring System (IMS), 1:254
International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), **2:139–140**
international crime efforts, 2:139
publications of, 2:139
International Space Station, 3:97
Internet, **2:140–143**
anti-spam legislation, 2:144
ARPANet and Internet history, 2:141–142
chat rooms and email, 2:148
commercial networks on, 2:142
guerilla tactics on, 2:75
ISP client information and Patriot Act, 1:387
WWW browsers, 2:142
Internet security threats
cyber attack and security, 1:301
hacking and cyber-crimes, 1:300, 2:142–143
surveillance, 2:145–147
Internet service providers (ISPs), 2:142
Internet spam and fraud, **2:144**
Internet spider, **2:144–145**
Internet surveillance, **2:145–147**
Electronic Communications Privacy Act (1994), 2:146
Internet technologies
IP addresses, 2:142, 2:143
protocols, 1:305, 2:141
tracking tools, 2:147–148
wireless, 1:300
Internet tracking and tracing, **2:147–148**
INTERPOL (International Criminal Police Organization), **2:148–149**
INTERPOL, U.S. National Central Bureau, **2:150**
Interrogation, 2:*151,* **2:151–152**
See also Torture techniques and technologies
Invisible ink, 3:58
Ionizing radiation, 2:244
IRA. *See* Irish Republican Army (IRA)
Iran
American hostages in, 1:166, 2:158–160, 2:274
biological weapons in, 1:114
IAEA inspectors in, 2:161
nuclear programs in, **2:160–161**
Shah of Iran and U.S., 2:273–274
Iran-Contra affair, 1:30, **2:155–157,** 2:274
conspiracy trials, 1:214, 1:331
Iranian hostage crisis, **2:158–160,** 2:*159,* 2:274
Iran intelligence and security, **2:157–158**
Iran-Iraq war, 2:275
nerve gas use in, 2:322
Iraq
American intelligence on, 2:416
anthrax production, 1:36–37
biological weapons in, 1:5, 1:114, 1:*115,* 1:334
botulism toxin in, 1:139
chemical weapons in, 2:165
intelligence and security agencies in, **2:161–162**
looting of national museum, 1:47
propaganda in, 1:334
weapons inspections in, 2:162–167
Iraq wars, **2:169–176,** 2:*170*
prelude to, **2:162–167**
aftermath, **2:167–168**
civil demonstrations for peace, 2:165
communication centers bombing, 2:*171*
media coverage of, 2:175
psychological warfare in, 2:173–174
Ireland, intelligence and security, **2:176–177**
Irish Republican Army (IRA), **2:177–178**
Iris scans, 3:16–17
IRS. *See* Internal Revenue Service (IRS)
IRS Restructuring and Reform Act (1998), 2:137
ISACs. *See* Information Sharing and Analysis Centers (ISACs)
Islamic Army of Aden (IAA), **2:178**
Islamic fundamentalism, 1:331
in Middle East, 2:273–274
Islamic Movement of Uzbekistan (IMU), **2:178–179**
Islamic Resistance Movement (HAMAS), **2:77**
Islamic Union. *See* Al-Ittihad al-Islami (AIAI)
Isotopic analysis, **2:179–180**
Israel
Arab-Israeli wars, 2:273
counter-terrorism policy, **2:180–181**
intelligence and security, **2:181–183**
Palestinian conflict and terrorism, 3:*149*
Pollard espionage case, 2:430–431
USS Liberty incident, 3:218–220
Yom Kippur War, 2:284
ITA. *See* Intelligence and Threat Analysis (ITA)
Italy, aircraft carrier development, 1:19–20
Italy, intelligence and security, **2:183–184**

I J I

Jackson, Henry, 2:198
Jackson Subcommittee
Kennedy and NSC, 2:198
Jaish-e-Mohammed (JEM) (Army of Mohammed), **2:185**
Janjalani, Abdurajak Abubakar, 1:1–2
Janjalani, Khadaffy, 1:2
Japan
aircraft carrier development, 1:19
espionage of Pearl Harbor, 2:412
intelligence and security, **2:186**
Manchuria takeover by, 2:411
Purple cipher machine, 2:459–460, 3:185
trade embargo on, 2:411–412
Japanese-American internment camps, 2:7, 2:122
Japanese Red Army, **2:186–187**
JDAM (Joint Direct Attack Munition), **2:187–188**
Jedburghs (WWII), 2:390
Jeffereys, Dr. Alec, 2:435
Jefferson, Thomas, 1:28
cipher wheel development, 1:289
Jemaah Islamiya (JII), **2:188**
Jenner, Edward, 3:85, 3:221, 3:227
Jerusalem
U.N. declared international city, 2:181
Jihad Group, 1:25
Johnson, Clarence L., 3:82
Johnson administration (1963–1969)
Dominican Republic intervention, 1:29
national security, **2:188–189**
National Security Council, 2:*356*–357
Tonkin Gulf Resolution, 2:189, 3:233
Vietnam war, 1:237
Johnston, Philip, 3:264
Joint Chiefs of Staff, U.S., **2:190,** 2:*191*
Joint House-Senate Intelligence Committee, 2:*129*
Joint Task Force on Intelligence and Law Enforcement, 2:127
Jonze, Spike (film director), 1:260
Jordan, intelligence and security, **2:191–192**
Joyce, William (Lord Haw-Haw), 2:238–239
J-STARS (Joint Surveillance and Target Acquisition Radar System), **2:192–193**
Judge advocate general (JAG), 2:276
Judiciary Act (1789), 2:193
Justice Department, U.S., **2:193–195,** 2:*194*
crime rate trends, 2:194–195
history, 2:193

intelligence agencies in, 3:204

K

Kabila, Laurent, 1:7
Kahane Chai (Kach), **2:197**
Karzai, Pres. Hamid (Afghanistan), 1:*60*
Keeler, Leonarde, 2:433
Kelly, David, 2:168
Kennan, George, 1:234
Kennedy, John F., 1:29
  assassination, 3:57
  Bay of Pigs (Cuba), 1:96, 1:97–98, 1:293–295, 2:198
  Berlin Wall, 1:105
  Continuity of Government program (COG), 1:269–270
  Cuban Missile Crisis, 1:252, 1:292, 1:*294*, 2:*198*
  missile gap with Soviet Union, 1:237, 2:198
  Peace Corps, 2:198
Kennedy, Philip (robotics scientist), 1:140
Kennedy administration (1961–1963)
  containment of Soviet expansionism, 2:197
  Jackson Subcommittee and NSC, 2:198
  military force buildup, 2:199
  National Security Council, 2:356–357
  national security policy, **2:197–199**
Kenya
  bombing of U.S. Embassy, 2:*200*, **2:200–201**
Keyhole intelligence satellites, 1:187, 1:310, 2:60, 3:15
  Imagery intelligence (IMINT) source, 2:100, 2:248
KGB (Soviet Union), **2:201–203**, 3:30–31
  Berlin Tunnel, 1:102
  crime prevention control, 1:280–281
  dirty tricks, 1:331
  forgery operations, 1:347–348
  SMERSH (KGB assassination team), 1:63–64, 2:202
  surveillance cameras in, 1:156–157
  tactics of, 2:202–203
  use of double agents, 2:203
Khmer Rouge, 2:*154*
Khobar Towers bombing incident, **2:204**, 2:*205*
Khomeini, Ayatolla R., 2:*159*
Khruschchev, Nikita (Soviet Premier), 1:293–295
  Berlin and Germany political issues, 1:105–106
  Berlin Tunnel, 1:102
  U-2 incident, 3:179
KH satellite series, 1:187
KH series cameras, 1:155–156
Kilby, Jack (engineer), 2:266
Kilpatrick speech forgery, 1:348
King, Jr., Martin Luther, 2:8
Kissinger, Henry, 1:238, 2:30, 2:309, 2:334
  National Security Council, 2:357
  as Secretary of State, 1:325
Kitty Hawk (aircraft carrier), 1:*18*, 1:19
Klaproth, Martin Heinrich, 3:211
Knives and edge weapons, 1:64, **2:205–206**, 2:*206*
Koestler, Arthur, 1:3
Korea, North, 3:*43*
  China, nuclear technology and, 1:189
  intelligence and security, **2:346**
  nuclear capability estimates, 2:348–349
  nuclear weapons programs, **2:346–350**
  Pueblo hijacking incident, 2:456–458, 3:77
  restricting nuclear program inspections, 2:346–349
  Soviet communications with, 2:456
Korea, South, 2:209
  intelligence and security, **3:93**
Korean War, 1:234, **2:206–210**
  Army Security Agency (ASA, U.S.), 1:56
  China involved in, 1:379, 2:208
  Epidemiological Intelligence Service development, 1:168
  Soviet disinformation in, 1:332
Kosovo, NATO intervention of, **2:210–211**
Ku Klux Klan, 3:143
Ku Klux Klan Act (1871), 2:122, 3:143
Kumpulan Mujahidin Malaysia (KMM), **2:211–212**
Kurdistan Workers' Party, **2:212**
Kurtz, Michael J., 1:216
Kuwait Oil fires, **2:212–214**, 2:*213*
Kuztnetsov (aircraft carrier), 1:20

L

Lake, Anthony (NSC), 1:217
Land mines clearance programs, **3:190–192**, 3:*191*
Land Remote Sensing Policy Act, 3:43
LANDSAT satellite program, 1:187, 2:60, 2:425
Langley (aircraft carrier), 1:19
Langmuir, Irving, 2:259
Language education training and skills, **2:215–216**
Laporte, Pierre (Canadian state minister), 1:160, 1:162
Large Volume Radiation Detector, 1:144
Larson, John A., 2:433
Laser, **2:216–218**
  LIDAR, 2:217–218
  listening devices, **2:218**
Laser guided weapons, 1:*400*, 2:1, 2:217
Laser radar, 1:390
Laser weapons, 1:399
Lashkar-e-Tayyiba (LT) (Army of the Righteous), **2:218–219**
Laskar Mujahidin, 3:*152*
Latin America
  communism in, 1:238–239
  drug war and gangs in, 1:30–31
  IMF focus on, 2:99
  nationalism during Napoleonic wars, 2:281–282
  U.S. Army School of the Americas, 1:29
  U.S. security policy and interventions, 1:28–31
Launch vehicles, expendable, 2:298–299
Law enforcement
  Australia, 1:72
  ballistic fingerprints, 1:85
  CIA and, 1:281
  federal training centers, 2:222–224, 2:303–304
  International Narcotics and Law Enforcement Affairs, U.S. Bureau of (INL), 2:139–140
  providing intelligence to, 2:126
  psychotropic drugs and, 2:454–455
  responses to terrorism, 2:219–222
  surveillance systems, 1:220–221
Law enforcement Partnership to Combat Terrorism Act (2002), 2:222
Law Enforcement Training Center, U.S. Federal (FLETC), **2:222–224**, 2:*223*
Lawrence, Ernest Orlando, 2:224
Lawrence Berkeley National Laboratory (LBL), **2:224–225**
Lawrence Livermore National Laboratory (LLNL), 2:44, **2:225–226**
  high power microwave weaponry, 2:272
  L-Gel decontaminant, 2:230–231
  nucleic acid analyzer, 2:379
Lazar, Robert, 1:51
League of Nations, **2:226–227**
Lebanon, bombing of U.S. embassy and barracks, **2:227–228**
Lebed, Alexander (Soviet diplomat), 1:173
Lee, Gen. R. E., 1:211, 1:212
Leeuwenhoek, Anton van (Dutch naturalist, 1660's), 1:80
Left-wing terrorists, 3:144–145
Lenin passport forgery, 1:*345*
Less-lethal weapons technology, **2:229–230**, 2:*230*
Leventhal, Todd, 1:334
Lew, Elizabeth Van, 1:212
Lexington (aircraft carrier), 1:19
L-Gel decontamination reagent, 1:317–318, **2:230–231**
Liberation Tigers of Tamil Eelam (LITE), **2:231–232**
Liberia, ethnic oppression in, 1:8
Libicki, Martin C., 2:107
Libraries and Information Sciences, U.S. National Commission on (NCLIS), **2:232**

Libya
intelligence and security, **2:233**
PanAm 103 bombing and trial of Libyan agents, 2:398–400
support of terrorist groups, 2:275
U.S. attack of (1986), **2:233–234**
Libyan Fighting Group, 1:25
Libyan Islamic Fighting Group, 1:25
LIDAR (Light detection and ranging), 2:217–218, **2:234–235,** 3:*14*
Life Support for Trauma and Transport (LSAT), 1:120
Limited Test Ban Treaty, 1:253
Listening devices, 1:145–147
Electronic Communication Privacy Act (1986), 1:146
noise generators, 2:341
Litvinenko, Alexander, 2:*131*
Lloyd, William Alvin, 3:206–207
Lockheed Martin Aeronautics Company
Skunk Works, 3:82–83
Lockpicking, **2:235**
Locks and keys, **2:236**
Lombroso, Cesare, 2:433
Lonetree, Clayton J., 3:74–76
Long, Breckinridge (Dept. of State), 1:198
Long, John, 1:*164*
Long Duration Exposure Facility (LDEF), 2:320
Looking Glass (Airborne Command Post), **2:237,** 2:*238*
"Loose nukes," 3:32–33
Loral Space and Communications Corp., 1:322, 3:42
Lord Haw-Haw (William Joyce), **2:238–239,** 2:450
Lord's Resistance Army (LRA), **2:239**
Los Alamos National Laboratory (LANL), **2:239–241**
supercomputer at, 2:*240*
Wen Ho Lee, 1:190, 1:191, 1:213, 2:133
Los Angeles International Airport, 1:*21*
Los Angeles Olympics leaflet forgery, 1:348
Louvre Museum (France)
protection of art and antiquities, 1:46, 1:47
Lowe, Thaddeus, 1:92
Loyalist Volunteer Force (LVF), **2:241**
LSAT. *See* Life Support for Trauma and Transport (LSAT)
Lugar, Richard, 3:32
Luminoso, Sendora, 1:31
Lumumba, Patrice (Congo Prime Minister), 1:7, 1:108, 1:237
Luria, A.R., 2:433

M

MacArthur, U.S. Gen. Douglas, 1:234
Korean war, 2:208
MacCracken, Jr. William P., 2:2
MacDonald, Sir John A. (Canadian Prime Minister), 1:161
Machiavelli, Niccolo, 1:418
Maclean, Donald, 1:153
MAD. *See* Mutually Assured Destruction (MAD)
Mad man theory, Richard Nixon, 1:238
Magaw, John, 3:*104*
Magnetic resonance imaging (MRI), 1:141
Mail sanitization, **2:243–245,** 2:442
Malicious data, **2:245**
Manchuria, Japanese takeover of, 2:411
Mandela, Nelson, 1:8
Maneuverable reentry vehicles (MARV), 1:89–90
Manhattan Project, 1:231, **2:245–247,** 2:*246,* 2:375
Oak Ridge National Laboratory (ORNL), 2:381
security for, 2:247
Mann Act (1910), 2:6
Mao Tse Tung (Mao Zedong, Chinese leader), 1:233, 2:208
Maps and mapping technology, **2:248**
bathymetric, 1:95–96
Geographic Information Systems (GIS), 2:64–65
National Imagery and Mapping Agency (NIMA), 2:331
Marine mammal program, **2:249–251**
Marine Mammal Systems (MSS), 2:251
MSS deployments, 2:251
Marines, U.S.
National Maritime Intelligence Center, 2:336–337
Marine traffic monitoring
U.S. Coast Guard, 1:221–222
Maritime Security Act (2002), 2:438–439
Markov, Georgi, 1:63–64, 1:107
Marshall, George (1880–1959), 1:232
as Secretary of State, 1:325
Marshall Plan (1947), 1:232, 1:233
Marston, William M., 2:433
Martial law
Posse Comitatus Act (1878) and, 2:126
Reconstruction period (1865–1877), 2:126
Martin, Archer, 2:49
Martin, Kate, 2:*27*
Maskhadov, Pres. Aslan (Chechnya), 1:173
Mass spectrometry, 2:38
Mathematical modeling
software for, 1:259–260
Matthei, Heinrich, 2:52
Maugham, W. Somerset, 2:262
Maxim, Hiram P., 3:80
Mayaguez (U.S. merchant ship)
communist capture of, 2:30
McCain, John S. (U.S. senator), 1:4
McCarthy, Timothy J., 3:*56*
McCarthy, U.S. Sen. Joseph, 1:233–234, 1:235, 2:123, 2:207, **2:251–253**
McClellan, Gen. G.B. (U.S. Civil War), 1:211, 1:212
McCone, John A., 1:195–196, 1:201, 1:310, 3:208
McFarlane, Robert C., 2:156
McGonagle, Comm. William, 3:218
McNamera, Robert S., 1:327, 2:189
McVeigh, Timothy, 3:144
Measures and Signatures Intelligence (MASINT), **2:253–254**
Medical Research Institute of Chemical Defense, U.S. Army (USAMRIDC), **3:213–214**
Medical Research Institute of Infectious Diseases, U.S. Army (USAMRIID), 3:*214,* **3:214–216**
Medical science resources
Centers for Disease Control and Prevention (CDC), 1:168–170
dual use technologies, 1:365
Epidemiological Intelligence Service, 1:168
infectious diseases, 1:170
LBL research in, 2:224
Meeks, Elsie (Civil Rights Commission), 1:*247*
Meitner, Lise, 2:22
Menzies, Stewart, 2:262
Merer, RAF Air Comm. J.F., 1:100
Metal detectors, **2:254–256,** 2:*255*
Meteorology
measuring instruments, 2:256
satellites, 2:257
weather alteration and, **2:256–260**
Meusnier, Jean-Babtiste-Marie, 1:93
Mexico
intelligence and security, **2:260**
Pancho Villa, 1:28
MI5 (British Security Service), **2:260–261,** 3:194
Cambridge University Spy Ring, 2:261
Suez crisis, 1:404–405
work against German and Soviet infiltrators, 2:261
MI6 (British Secret Intelligence Service), **2:262,** 2:*263,* 3:195
Bletchley Park cryptanalysis, 2:262
Microbiology
applications of, **2:263–266**
genetic detection and identification, 2:265
Microchip, **2:266–267**
Microdot cameras, 1:159–160
Microelectronics, 2:461
Microfilms, **2:267–268,** 2:*268*
Microorganisms as biological weapons, 2:264–265
Microphones, 1:146, **2:268–270,** 2:*269,* 3:78
parabolic, 2:403
types of, 2:268–269

Microprocessors, 2:266
bio-flip implants, 1:112
Moore's Law, 2:266–267
Microscopes, **2:270–271**
Microwave weaponry
high power, **2:271–272**
Middle East
anti-American sentiment in, 2:66
espionage in ancient, 1:416
independence of nations, 2:273
Islamic fundamentalism, 2:273–274
rise of terrorism in, 2:272–273
Soviet incursions in, 1:233
U.S. defense against communism, 1:237
U.S. security policy and interventions, **2:272–275**
Middle East oil
U.S. dependency on, 1:147, 1:166
Midway, battle of, 1:19
Military aircraft testing facility, 1:51
Military intelligence
Germany, 1:74
Russia, 1:74
United States, 1:243–244, 1:327–329, 2:47
use of terrain intelligence, 2:58–59
Military Joint Intelligence Center (NMJIC), United States, 1:327
Military personnel
anthrax vaccine, 1:37, 1:39
Berlin Airlift operations, 1:100–101
Persian Gulf War arsenal, 2:415–416
Special Forces, 1:322
Military police, U.S., **2:276**
Milosevic, Slobodan, 2:210
Ming Zhong, 1:373
Miniature cameras, **1:157–160**
microdot camera, 1:159–160
Minox camera, 1:265–266, 2:267
pinhole camera, 1:158
Tokya 78-M (Soviet), 1:157
video camera, 1:*158*
wristwatch cameras, 1:159
Mini-Ramen LIDAR System (MLRS), 1:143
Minox camera, 1:158–159, 1:265–266, 2:267
Minuteman ICBM (U.S.), 1:*87,* 1:90, 2:*374*
MIRV (Multiple independently targetable reentry vehicle), 1:89, 1:90, 2:30
Missile defense lasers, 2:217
Missiles
categories of, 1:89
flight profile, 1:89–90
payloads and warheads, 1:90
Mitnick, Kevin, 1:*257*
MOAB (Massive Ordnance Air Burst Bomb), **2:276–278,** 2:*277*
Mobilization Against Terrorism Act (MATA), 2:114
Mobutu, Joseph Désiré, 1:6
Mohammed, Khalid Sheikh, 1:49
Molecular biology applications, **2:278–279**
Moles, **2:279–281**
Molotov Plan (Soviet Union), 1:232
Monge, Gaspard (18th century mathematician), 1:259
Monroe Doctrine, 1:28, **2:281–282**
Montague, Lady Mary Wortley, 3:221, 3:227
Montes, Ana B., 1:292
Montgolfier, Jacques-Etienne (French balloon pilot), 1:92
Montgolfier, Joseph-Michel (French balloon pilot), 1:92
Moore, Gordon (engineer), 2:266–267
Moore's Law (microchip electronics), 2:266–267
Morgan, John Hunt (Confederate Calvary), 1:211
Morgenthau, Henry, 3:170–171
Morocco, intelligence and security, **2:282–283**
Moro National Liberation Front, 1:1–2
Morse, Samuel F. B., 1:289, 1:419
Morse code, 1:*225,* 1:289, 1:419
Mossadegh, Mohammed (Iranian Premier), 1:195
Mossad (Israeli Institute for Intelligence and Special Tasks), 2:*283,* **2:283–284**
resources and organization, 2:284
Wrath of God team response to Munich Olympics, 2:283–284
Yom Kippur War, 2:284
Mössbauer spectroscopy, 3:108
Most, Johann (1846–1906), 3:150
Motion sensors, **2:284–285**
Mountin, Dr. Joseph M. (CDC director), 1:168
Mount Weather (COG safety site), **2:285–286**
Movies
Alfred Hitchcock and spy, 2:286
"Dr. Strangelove," 2:*287*
espionage and intelligence portrayals, **2:286–289**
ethnic portrayals in, 2:289
James Bond series, 2:287–288
terrorism in, 2:289
Mozambique, 1:8
MPLA. *See* Popular Movement for the Liberation of Angola (MPLA)
Mujahedin-e-Khalq Organization (MEK or MKO), **2:290**
Mullany, Pat, 2:449
Mullis, Kary B., 2:433
Multispectral imagery, 2:60, 2:248
Munitions, unexploded ordnance clearance programs, 3:190–191
Mussolini, Benito, 3:276
Mustard gas, **2:290–291,** 2:*291*
Mutually Assured Destruction (MAD), 1:42, 2:189
Myers, Gen. Richard B., 1:*306*

N

Nagasaki (Japan), 1:231, 2:23, 2:246
NAILS (National Automated Immigration Lookout System), **2:293**
Nanotechnology, **2:294–296**
applications in, 2:295–296
genetic studies, 2:56
National Nanotechnology Initiative, 2:296
quantum physics and, 2:294–295
Napoleonic wars
espionage during, **2:296–298**
Latin American nationalism during, 2:281–282
Narcotics. *See* Drugs and narcotics
NASA (National Aeronautics and Space Administration), **2:298–299**
airline security, 1:141
creation of, 1:237
DARPA programs transferred to, 1:306
hypersonic aircraft, 2:91
Mars Pathfinder mission, 3:26
Nassar, Pres. Gamel (Egyptian)
Baghdad Pact, 1:237
Soviet ties and Suez canal crisis, 1:404–405, 3:127
Nassr Engineering Manufacturing facility (Iraq), 1:*351*
National Advisory Committee for Aeronautics (NACA), 2:90
National Aeronautics and Space Administration. *See* NASA
National Airspace System (NAS), 2:3
National Archives Act (1934), 2:300
National Archives and Records Administration (NARA), **2:300**
declassified information received by, 1:216
National Center for the Analysis of Violent Crime (NCAVC), 2:448–449
National Command Authority, **2:300–301**
National Communications System, U.S., **1:252**
National Contingency Plan (NCP), 1:394
National Counterintelligence Policy Board, 1:324
National DNA Database (NDNAD), 1:85
National Drug Intelligence Estimate (NDIE, Canada), **1:363**
National Drug Threat Assessment, **2:301**
National Firearms Act (1934), 1:68
National Imagery and Mapping Agency (NIMA), 2:60, 2:248, **2:331**
declassified documents, 1:216
Photographic Interpretation Center (NPIC), 2:423
National Information Infrastructure Protection Act, U.S. (1995), **2:301–302**
National Institute of Justice (NIJ), **2:330**
National Institute of Mental Health (NIMH), **2:332**

How to go to your page

National Institute of Standards and Technology (NIST), 1:*245,* 1:246, **2:332–333**
Computer Security Division, 2:333–334
National Institutes of Health (NIH), **2:329–330,** 2:455
BioShield Project, 1:123
protective measures development, 1:126
National Integrated Ballistics Identification Network, 1:85
National Intelligence Council, **2:325–326**
National Intelligence Estimates (NIEs), 1:324, **2:302–303,** 2:325
criticism of, 2:303
National Interagency Civil-Military Institute, U.S. (NICI), **2:303–304**
National Liberation Army (ELN), **2:304**
National Military Joint Intelligence Center, **2:305**
National Missile Defense (NMD), 3:124–125
National Money Laundering Strategy (NMLS), 3:156–157
National Nanotechnology Initiative, 2:296
National Nuclear Security Administration (NNSA), **2:337–340**
National Oceanic and Atmospheric Administration (NOAA), **2:340–341**
Cospass- Sarsat satellite system, 2:341
National Weather Service, 2:340
National Pharmaceutical Stockpile Program (NPS), 1:126, 1:319
National Preparedness Strategy, U.S., **2:305–306**
National Reconnaissance Office (NRO), **2:350–351,** 3:46
National Response System, 1:394
National Response Team, U.S., **2:306–307**
National School of Biological Sciences (Mexico), 1:*184*
National Science Foundation (NSF), 2:141–142, **2:360**
National Security Act (1947), 1:193, 1:200, 1:202, **2:307–308**
Truman presenting to Congress, 1:234
National Security Advisor, U.S., **2:308–310,** 2:354
National Security Agency (NSA), **2:351–353**
careers in, 2:120
document declassification, 1:215–216
secrecy of, 2:351–252
National security and emergency preparedness (NS/EP), 1:252
National Security Council (NSC), 1:*149,* **2:353–355,** 2:*354*
Clinton administration, 1:*217*
Cold War operations, 1:232
history of, 1:200, **2:355–359**
Kennedy and Jackson Subcommittee, 2:198
memorandum 68, 1:234
republican administrations, 2:353–354
U.S. President and, 2:444–445
National Security Strategy, U.S., **2:310–311**
National Security Telecommunications Advisory Committee, **2:311**
National Telecommunications Information Administration, U.S. (NTIA), **2:312**
National Transportation Safety Board (NTSB), **2:360–362**
National Union for the Total Independence of Angola (UNITA), 1:8
National Weather Service, 2:257, 2:340
NATO (North Atlantic Treaty Organization), **2:312–314,** 2:*313*
Berlin Wall, 1:103
deterrence strategies to biological warfare, 1:125–126
formation of, 1:232, 1:233
Kosovo intervention, 2:210–211
Natural resources, national security, **2:314–315**
Navaho Indians (Code-talkers), 1:291, 3:263–265
Navigational satellite systems
GPS (Global Positioning System), 2:68–70
Navstar, 2:68
Navigation tools, 2:68–69
Navstar, 2:68
Navy, U.S.
aircraft carrier development, 1:19
NMIC (National Maritime Intelligence Center), 2:336–337
Pueblo incident and Project Clickbeetle, 2:456, 3:77
ships designed for intelligence collection, **3:76–77**
Navy Criminal Investigation Service (NCIS), **2:316**
Nazi Germany
art and antiquities "Great Theft," 1:47
Gestapo and Abwehr, 1:3
Nazi Security Service, 1:2
propagandist for, 2:238–239
psychological warfare in, 2:108–109
NCIX (National Counterintelligence Executive, U.S. Office of the), **2:317–318**
NCLIS. *See* Libraries and Information Sciences, U.S. National Commission on (NCLIS)
NDIC (National Drug Intelligence Center, Dep't of Justice), 2:*318,* **2:318–319**
NDNAD. *See* National DNA Database (NDNAD)
Near-space environment, **2:319–321**
Long Duration Exposure Facility (LDEF), 2:320
nuclear devices in, 2:319–320
Nebel, Fritz, 1:4
Nechaev, Sergei (1847–1882), 3:150
Nedrow, Roy D., 2:316
Nellis Air Force Base (U.S.), 1:51
Nerve gases, **2:321–322,** 2:*322*
G and V agents, 2:322
Soman, 3:89–90
Tabun, 2:321–322, 3:133
VX nerve agent, 3:246–247
NEST. *See* Nuclear Emergency Support Team (NEST)
Netherlands, intelligence and security, **2:323**
New People's Army (NPA), **2:323–324**
Newsham, Margaret, 1:372
News media, war coverage, 1:305
New Zealand, intelligence and security, **2:324**
NFIB (National Foreign Intelligence Board, U.S.), **2:325**
Ngo Dinh Diem (S. Vietnam Prime Minister), 1:237, 3:232
Nicaragua
Communists in, 1:196
Contras and Sandinistas in, 1:30
intelligence and security, **2:326–327**
occupation of, 1:28
See also Iran-Contra affair
Nichols, Terry, 3:144
Nicolai, Walther, 1:2
Nigeria
intelligence and security, **2:327**
police force and criminal activity in, 1:9
Night vision scopes, **2:327–329,** 2:*328*
image intensification, 2:327–328
infrared imaging, 2:111–112, 2:328–329, 2:382
NIH (National Institutes of Health), **2:329–330,** 2:455
BioShield Project, 1:123
protective measures development, 1:126
Nimitz class aircraft carriers, 1:18, 1:19
NIPC. *See* Infrastructure Protection Center, U.S. National (NIPC)
Nirenberg, Marshall, 2:52
NIST (National Institute of Standards and Technology), 1:*245,* 1:246, **2:332–333**
Computer Security Division, **2:333–334**
Nixon, Richard M., 1:237–238
Chile intervention, 1:29
China visit, 1:238, 2:335
kitchen debate with Khruschchev (as V.P), 1:235
redefining Cold War—Nixon Doctrine, 1:237–238
stopped biological weapons research, 1:116
Nixon administration (1969–1974), **2:334–335**
National Security Council, 2:357
Security Council, 2:*335*
Vietnam withdrawal, 3:234

Watergate scandal, 1:202, 2:335
NMIC (National Maritime Intelligence Center), **2:336–337**
Marine and Coast Guard components, 2:337
Naval components of, 2:336
Office of Naval Intelligence (ONI), 2:336–337
NNSA (National Nuclear Security Administration), **2:337–340**
NOAA. *See* National Oceanic and Atmospheric Administration (NOAA)
Noble, Ronald (INTERPOL), 2:*149*
Noise generators, **2:341**
Non-governmental global intelligence and security, **2:342–343**
Nonproliferation and national security, U.S., **2:343**
Non-Proliferation Treaty (NPT)
North Korea and NPT Safeguards agreement, 2:349
Nonproliferation Verification Research and Development Program (NNSA), 2:339
NORAD (North American Air Defense Agreement), 2:*344,* **2:344–346,** 2:*345*
drug smuggling and trafficking and, 2:345
Noriega, Manuel (Panamanian dictator), 1:29, 1:30, 1:279, 1:310, 2:109
North, Oliver, 2:*155,* 2:156, 2:358
North Atlantic Treaty Organization (NATO), **2:312–314,** 2:*313*
Berlin Wall, 1:103
deterrence strategies to biological warfare, 1:125–126
formation of, 1:232, 1:233
Kosovo intervention, 2:210–211
North Korea. *See* Korea, North
Northrop Grumman, B-2 Bomber, 1:79
Norway, intelligence and security, **2:350**
Norwood, Melita, 1:*230*
Noyce, Robert (engineer), 2:266
NPIC. *See* Photographic Interpretation Center, U.S. National (NPIC)
NPS. *See* National Pharmaceutical Stockpile Program (NPS)
NRO (National Reconnaissance Office), **2:350–351**
NSA. *See* National Security Agency (NSA)
NTA. *See* Anti-imperialist Territorial Nuclei (NTA, Italy)
NTTC. *See* Technology Transfer Center, National (NTTC)
Nuclear, biological, and chemical defense, Surgeon General and, **3:129–130**
Nuclear arms control, 2:366
dismantling, 1:321
International Monitoring System (IMS), 1:254
START I Treaty, **3:112–113**
START II Treaty, 3:*113,* **3:113–114**
verification of, 1:254
Nuclear Emergency Support Team (NEST), 2:239–240, 2:*363,* **2:363–364,** 2:*364*
Nuclear Fission, **2:22–24,** 2:365–366
Nuclear Fusion, **2:44–46,** 2:375
as energy source, 2:45–46
fusion sequence, 2:44–45
Nuclear magnetic resonance, 3:108
Nuclear materials
byproducts and waste, 2:369–370, 2:371, 2:381
decontamination, 1:318, 1:321
safeguarding, 3:255–256, 3:257
tracking methods, **3:256–257**
Nuclear power plants, **2:365–368**
aircraft carriers, 1:19
Chernobyl, 1:68, 1:185–188
dependent on heavy water development, 2:82–83
first reactor for energy production, 2:23
public perception of, 2:372
security of, 2:365–368
Three Mile Island, 1:68, 2:*365,* 2:372
Nuclear proliferation, 2:365
nonproliferation, 2:343, 2:377
nuclear arms race, 1:166–167, 2:375
Nuclear reactors, 2:23, 2:*368,* **2:368–370**
naval, 2:370
neutron moderation in, 2:82
nuclear chain reactions, 2:246
satellite mishaps with, 2:319–320
Nuclear Regulatory Commission (NRC), **2:370–372,** 2:*371*
Nuclear safety and security
Argonne National Laboratory, 1:53
dismantling, 1:321, 3:32
DOE office of security, 1:353
National Nuclear Security Administration, 2:337–340
Nuclear Emergency Support Team, **2:363–364**
radiation detectors, **2:362–363**
threat assessment, 2:339, 2:367, 3:32–33
Nuclear spectroscopy, **2:372–373**
Nuclear testing
Comprehensive Test Ban Treaty (CBT), 1:253–254
Limited Test Ban Treaty, 1:253
Threshold Test Ban Treaty, 1:253–254
U.S. and Russia announces testing moratorium, 1:254
Nuclear warfare, nuclear winter theory, 2:376–377, **2:378–379**
Nuclear weapons, **2:374–378**
biological damage from, 3:3–4
certification and testing of, 2:225–226
declassified information mistake, 1:191
LLNL research in, 2:225–226
"loose nukes," 3:32–33
Manhattan Project, 2:245–247
radiation detectors, 2:362–363
Russian security of, 3:31–33
smuggling of, 2:339
types and sizes of, 2:377
Nucleic acid analyzer, **2:379–380**
Number theory, cryptography and, 1:286–287
Nunn, Sam, 3:32
Nunn-Lugar Threat Reduction Program, 3:32
Nye, Jr., Joseph S., 2:303

101

Oak Ridge National Laboratory (ORNL), **2:381–382,** 2:*382*
chemical-biological mass spectrometer (CBMS), 2:179, 2:381
Ocean mapping. *See* Bathymetric maps
Office of Naval Intelligence (ONI), 2:336–337
Office of Research Reports (ORR, CIA), 1:374
Office of Strategic Services (OSS), U.S., 1:199–200, **2:389–391,** 3:208
use of silencers, 3:81–82
Office of the Surgeon General, U.S.
biomedical effects of nuclear, biological and chemical weapons (NBC), 3:129–130
Official Secrets Act, U.K. (1889, 1911, 1989), **2:382–384**
Ogorodnik, Aleksander, 1:298
Oil spills reporting, Coast Guard National Response Center, 1:223
OIS. *See* Information Security, U.S. Office (OIS)
Oklahoma City bombing, 1:134, 2:136, 3:144
Olympic Games
Munich 1972, 2:61, 2:283–284
Salt Lake City 2002 security, 2:435
Omnibus Diplomatic Security and Antiterrorism Act (1986), 2:438
OPEC. *See* Organization of Petroleum Exporting Countries (OPEC)
Open market operations
Federal Open Market Committee, 2:*13,* 2:14
Open source intelligence (OSINT), 1:199
Operation Allied Force (Kosovo), 2:210
Operation Desert Storm. *See* Persian Gulf War
Operation El Dorado Canyon (Libya), 2:234
Operation Enduring Freedom, **1:397–398,** 1:*398*
Operation Engulf (U.K.), **1:404–405**
Operation Green Quest, 1:296
Operation Iraqi Freedom, 1:149, 2:*169,* **2:169–176**
aftermath of, 2:167–168

aircraft in, 1:79, 1:80, 2:2
media coverage of, 2:175
missiles in, 1:*285,* 2:187
psychological warfare in, 2:109–110
shock and awe tactics in, 2:174
Operation Just Cause, 2:109
Operation Liberty Shield (Homeland Security), **2:385–386**
Operation Magic, **2:386–387**
Operation Mincemeat (WW II), 3:281–282, **3:282–283**
Operation Mongoose (Cuba), **2:387–388**
Operation Shamrock, **2:388–389**
Operation Torch (North Africa), 2:390
Operation Ultra, **3:184–185**
Operation Urgent Fury (Grenada), 1:29
OPIR. *See* Intelligence Policy and Review, U.S. Office of (OPIR)
Oppenheimer, J. Robert, 1:231, 2:23, 2:239, 2:246, 2:375
Orange Volunteers (OV), **2:389**
Organization of Petroleum Exporting Countries (OPEC), **2:384–385**
oil embargoes, U.S., 1:238, 2:384
U.S. national security and, 1:147, 2:315
Organized Crime Act (1970), 1:68
OSINT. *See* Open source intelligence (OSINT)
Ostrander, Sheila, 2:452
Ostrovsky, Victor, 1:157
Ottawa Convention (Land mine ban), 3:192
Ottoman Empire, 2:272–273
Outlying Area Reporting Station (OARS), 2:439
OV. *See* Orange Volunteers (OV)

P

P-3 Orion reconnaissance aircraft, **2:393,** 2:*394*
Pacific Northwest National Laboratory (PNNL), **2:394–395,** 2:*395*
PAGAD. *See* People Against Gangsterism and Drugs (PAGAD)
Painvin, Georges-Jean, 1:4
Pakistan, intelligence and security, **2:396–397**
Palestine Authority intelligence and security, **2:398**
Palestine Authority warfare summer camps, 2:*75*
Palestine Islamic Jihad (PLJ), **2:397**
Palestine Liberation Army (PLO), 1:1
Palestine Liberation Front (PLF), **2:397–398**
Palestine Liberation Organization (PLO), 1:61–62
Panama
Canal construction and history, 2:401
Noriega and intervention in, 1:30
Panama Canal Treaty, 2:401
Panama Canal, **2:401–403,** 2:*402*
U.S. transfer to Panama, 2:402
Panama Canal Commission, 2:402
Panama Canal Treaty, 2:401
PanAm Flight 103 bombing, **2:398–400,** 2:*399*
Parabolic microphones, **2:403**
Paranormal abilities, **2:451–453**
remote viewing experiments, 2:452
Para-state organizations, 3:151–154
Parks, Cliff, 3:*277*
Particle accelerators
at CERN, 1:*171*
Particle beam weapons, 1:399
Passenger screening
process, 1:21–22
for toxins, 1:5
Passive infrared systems (PIRs), 2:284–285
Pasteur, Louis, 1:81, 1:83
rabies vaccine, 3:223
Pasteurization, 1:81, 1:83
Pathogen genomic sequencing, **2:404**
Pathogens, **2:405–407**
transmission and spread of, 2:404–406
Pathogen transmission, **2:404–405**
Patriot Act, USA (2001), 1:386–387, 2:123, **2:408,** 2:*409,* 3:71
deterrence policy, 3:200
law enforcement intelligence under, 2:219–220
terrorist exclusion list, **2:407**
Patriot Missile System, **2:408–409,** 2:410
Payton, Gary (astronaut), 2:299
Pearl Harbor attack, 1:19, **2:410–413,** 2:*411*
Penicillin, 1:43
Penkovsky, Oleg, 2:281
Pennsylvania (battle ship), 1:19
Pentagon, 1:350–351, 3:*70*
hacker attack on, 1:256
underground facility, 1:283
Pen Yen Yang, 1:*373*
People Against Gangsterism and Drugs (PAGAD), **2:413**
People's Liberation Army (PLA, China), 1:189
People's Republic of China (PRC). *See* China
Peron, Pres. Juan Domingo (Argentina), 1:52
Pershing, Gen. John
pursuit of Pancho Villa, 1:28
Persian Gulf War, **2:414–416,** 2:*415*
DIA intelligence in, 1:327
Kuwait oil fires, 2:*213*
news media and, 1:305
psychological warfare in, 2:109
stealth aircraft in, 1:80, 2:1
Personal security and identification
dumpster diving, 1:299–300, 1:342, 2:96
name recognition software, 2:94
Personal Status Monitor (PSM), 1:119–120
Personnel security
Personnel Security Investigations (PSI), 1:321–322
Peru
aircraft carrier development, 1:19
election protest in, 1:*332*
intelligence and security, **2:417**
Peterson, S., 2:256
Petroleum Reserve, U.S.
determination of, 2:417–419
Nixon and, 2:384
strategic, **3:125–126**
Petroleum reservoirs, 2:418–419
PFIAB. *See* President's Foreign Intelligence Advisory Board (PFIAB)
PFLP. *See* Popular Front for the Liberation of Palestine (PFLP)
Pharmaceuticals
National Pharmaceutical Stockpile Program (NPS), 1:126, 1:319
Philby, Kim, 1:*152,* 1:152–153, 1:*361,* 2:203, 2:280
Philippines and the Spanish-American War, 3:102–103
Phoenix Program, **2:420–421**
Photo alteration, **2:421–423**
Photographic Interpretation Center, U.S. National (NPIC), **2:423–424**
Photographic resolution, **2:424**
Photography
digital alteration, 2:422–423
high-altitude, **2:424–426**
invention of, 1:419
traditional alteration, 2:421–422
PHS. *See* Public Health Service, U.S. (PHS)
Physics
electromagnetic spectrum, 1:381–382
nuclear, 2:375–376
spectrum, 1:382–383
Pickler, Nedra (reporter), 2:*96*
Pike, Otis (U.S. Congressman), 2.135
Pike Committee
congressional oversight of intelligence community, 2.135–136
Pincher, Chapman, 1:331
Pinkerton, Alan, 1:211, 3:207
Pinochet, Gen. Augusto (Chile), 1:29, 1:188
Planck, Maxwell, 2:294
Playfair, Lyon, 1:289, 2:426
PLF. *See* Palestine Liberation Front (PLF)
PLJ. *See* Palestine Islamic Jihad (PLJ)
PLO. *See* Palestine Liberation Army (PLO)
Plum Island Animal Disease Center, 2:*427,* **2:427–428**
Plutonium, 1:231
fuel for nuclear fission, 2:23

tracking nuclear materials, **3:255–257**
PNNL. *See* Pacific Northwest National Laboratory (PNNL)
Poindexter, John M., 2:156
Poland
intelligence and security, **2:428**
intelligence on Enigma cipher machine, 1:131–132
U.S.—Soviet relations in, 1:233
Political murders
by assassins or terrorists, 1:60–61, 2:34–35
Pollard, Jonathan J. (espionage case), 2:*430,* **2:430–431**
Polybius square, 1:3–**4**
Polygraphs, **2:431–433,** 2:*432*
Polygraph tests
types of, 2:432
Polymerase chain reaction (PCR), **2:433–436,** 2:*434*
genetic detection devices, 1:117, 2:56, 2:379
Pons, Stanley, 2:45
Pony Express, 2:442
Popp, Georg, 2:33
Popular Front for the Liberation of Palestine (PFLP), **2:436–437**
General Command (PFLP-GC), **2:437**
Popular Movement for the Liberation of Angola (MPLA), 1:8
Port Passenger Accelerated Security System (PORTPASS), **2:439–440,** 3:67–68
Ports and Waterway Act (1972), 2:437–438
Port security, **2:437–439**
Port Security Units (PSUs), USCG, 2:438
Portugal, intelligence and security, **2:440–441**
Posse Comitatus Act (1878), 2:126
Postal Reorganization Act (1970), 2:442
Postal Service, U.S. (USPS), **2:442–443**
emergency preparedness plan, 2:441–442
Postal security, **2:441–442**
Potassium iodide, **2:443**
Powell, Colin L.
biological weapons in Iraq, 1:114
as Secretary of State, 1:325
United Nations Security Council and Iraq, 2:165
Powers, Francis Gary, 1:76, 1:298–299, 2:425, 3:179–180, 3:*181*
POWs. *See* Prisoners of war (POWs)
Presidential candidates
intelligence briefings of, **2:429**
Presidential directives, 1:423, 2:309
Presidential review memorandum forgery, 1:348
President of the United States
as executive commander of intelligence agencies, **2:444–445**
President's Foreign Intelligence Advisory Board (PFIAB), **2:419–420,** 2:445
Pretty Good Privacy (PGP), 1:228, 1:287, 1:291, **2:446**
Primakov, Yvgeny, 1:*148*
Prisoners of war (POWs), 2:125
Privacy rights
Bill of Rights, 2:447
Echelon, 2:448
Fair Credit Reporting Act (FCRA), 2:448
Freedom of Information-Privacy Acts (FOIPA), 2:447–448
legal and ethical issues, 2:447–448
Privacy Act (1974), 2:447
Profiling, **2:448–450**
Progressive Animal Welfare Society (PAWS), 2:249
Prohibition Unit (ATF), 1:66
Project GENETRIX, 1:93–94
Projection radiography scanning, 3:51–52
Project Shield America, 1:296–297
Propaganda and psychological warfare
Nazi propaganda, 2:*451*
uses and psychology, **2:450–451**
protection of art and antiquities, 1:48
Protein sequencing, 3:73
Protocols of the Learned Elders of Zion forgery, 1:344–345
Pseudoscience intelligence studies, **2:451–453**
Psychic viewing, 2:452
Psychological warfare, 2:108–109
brainwashing, 2:209
Psychotropic drugs, **2:453–455**
Public buildings
building risk assessment software (RAMPART), 1:49
designing for security, 1:48–50
government building design, 1:49
Public communications
Echelon monitoring, 1:370–372, 2:448
microchips for secure private, 1:218
Public health response system, 1:248–252
Public Health Service, U.S. (PHS), **2:455–456**
Public safety
Coast Guard (U.S. CG), 1:221–222
Public surveillance
closed circuit TV systems, 1:220–221
Echelon, 1:370–372
Pueblo incident, **2:456–458,** 2:*457,* 3:77
Purification, air and water, 1:10–11, 1:127
Purple machine (Japanese cipher machine), **2:459–460,** 3:185

Q

Qadhafi, Muammar, 2:233–234
Quantum computing, 2:462–463
Quantum cryptography, 2:462
Quantum physics
espionage and intelligence applications, **2:461–463**
nanotechnology and, 2:294–295
particle entanglement, 2:461–462
teleportation, 2:462–463
QuickBird satellites, 3:*44*

R

R-7 ICBM (Soviet Union), 1:89
Raborn, William F., Jr. 1:196, 1:310
Radar, **3:1–2**
doppler effect, 3:2, 3:119
satellites, 3:49
stealth technologies, 3:117–118
synthetic aperture, 2:59, 2:60, 3:2–3
Radiation
biological damage, **3:3–4**
for decontaminating, 2:244
detectors, 2:224, 2:362–363
energy absorption measurement of, 1:359
ionizing, 2:244
Large Volume Radiation Detector, 1:144
from nuclear weapons, 2:376
Radioactive waste storage, 2:369–370, 2:381, **3:6–7**
Radio equipment
direction finding, **3:4–5**
radiometers for remote viewing, 1:390
RF detection, **3:23**
Radio frequencies
spectrum allocation, 1:383
waves as signals, 1:382
Radio frequency (RF) weapons, **3:5–6,** 3:23
Radiological Emergency Response Plan, U.S. Federal (FRERP), **3:8**
Radio Tokyo, 3:163–164
Al Rahman, Shaykh Umar Abd, 1:23
Raman spectroscopy, 3:108–109
Ranger (aircraft carrier), 1:19
Rasputin, Gregory Efimovich (Russian monk), 1:107
Raymond, Michael, 2:*280*
Reagan, Ronald
Angolan support, 1:8
assassination attempt., 1:*63,* 3:*56*
Computer Security Act (1987), 1:261
Iran-Contra affair, 1:30, 1:279, 2:155–157
Operation Urgent Fury, 1:29
South African apartheid, 1:8
Reagan administration (1981–1989)
drug war, 1:313
missiles in Western Europe, 1:240
National Security Council, 2:358–359
national security policy, **3:9**
Strategic Arms Reduction Treaty (START), 3:9

How to go to your page

Strategic Defense Initiative (SDI), 1:42, 3:9
Reagan signature forgery, 1:349
Real IRA (RIRA), **3:10–11**
Recombinant DNA, 2:56
experiments, 1:57, 1:58
genetic engineering of bacteria, 2:278–279, 2:406–407
Recombinant DNA experiments. *See* Asilomar Conference
Reconnaissance, **3:11**
Reconnaissance aircraft
Il'ya Mourometz bomber (Russian), 1:74
Skunk Works (Lockheed Martin), 3:82–83
SR-71 Blackbird, 1:76, 2:91, 2:425, 3:111–112
U-2 spy plane, 1:*74*
unmanned vehicles as, 1:76
World War II, 1:75
Reconnaissance satellites, 1:76, 2:248, 2:299
Red Code (Japanese naval code), **3:12**
Red Hand Defenders (RHD), **3:12–13**
Red Orchestra, **3:13**
Reid, John E., 2:433
Reid, Richard, 3:77
Reilly, Sidney, 2:262
Reinsch, William (Commerce Dep't), 1:365
Rejewski, Marian (Polish mathematician), 1:206, 1:407
Remote sensing, **3:13–15**
information source for terrain analysis, 2:59
LIDAR system and images, 2:234–235, 3:14
Remote sensing satellites, 1:187
commercial, 3:43–45
EM wave scanners, 1:392–393
EROS satellites, 3:43
IKONOS, 3:43
Land Remote Sensing Policy Act, 3:43
Landsat program, 2:425
QuickBird satellites, 3:*44*
Remote Video Inspection System (RVIS), 2:439–440
Remote viewing, 2:452
Renaissance, espionage in the, 1:418–419
Reno, Janet, 1:358
Republican Party resurgence, 1:233–234
Republican Sinn Fein (RSF), 1:267
Retina and iris scans, **3:15–17**
Revenue Acts (1916, 1917), 3:170
Revolutionary Armed Forces of Colombia (FARC), **3:18**
Revolutionary Nuclei, **3:18**
Revolutionary Organization 17 November (17 November), **3:19**
Revolutionary Organization of Socialist Muslims. *See* Abu Nidal Organization (ANO)
Revolutionary People's Liberation Party / Front (DHKP/C), **3:19**
Revolutionary Proletarian Initiative Nuclei (NIPR), **3:20**
Revolutionary United Front (RUF), **3:20**
Revolutionary War, American, 2:74, 3:06, **3:21–23**
Rewards for Justice Program, 1:276, 3:*153*
Rice, Condolezza, 2:*309,* 2:359
Richardson, Bill (U.S. Energy Secretary), 1:191
Richelson, Jeffrey T. (writer), 1:197, 1:372
Ricin, 1:107, **3:24,** 3:166–167
Ridge, Tom (Homeland Security director), 1:*124,* 2:*86,* 2:359
Operation Liberty Shield, 2:385–386
Ridgway, U.S. Gen. Matthew B., 2:208
Rintelen, Franz von, 1:130
Rivest, Ronald, 1:286
Robotics
brain-machine interfaces for, 1:140
energy harvesting and, 3:26–27
spacecraft and, 3:26
vehicles, **3:25–27**
Rogers, William, 2:358
Rohrbacher, Dana, 3:42
Roman Empire
espionage in the, 1:416–417
Romania, intelligence and security, **3:27–28**
Romerstein, Herbert, 1:349–350
Roosevelt, Franklin D., 1:198, 1:230
Roosevelt, Theodore
Rough Riders in Spanish-American War, 3:103
Rosario Cases, Maria Del, 1:31
Rosenberg espionage case (Ethel and Julius), 3:*29,* **3:29–30**
Rossignol, Antoine, 1:128
Rostow, Walt, 2:189
Rover race (DARPA sponsored), 1:306
Rowan, Andrew, 3:103
Rowley, Colleen, 3:71
Royal Canadian Mounted Police (RCMP), 1:160, 1:161
National Drug Intelligence Estimate (NDIE, Canada), 1:363
Royal Navy (U.K.), 1:19
RPF. *See* Rwandan Patriotic Front (RPF)
RQ-1 predator aircraft, 1:*27*
Rubin, Robert, 3:*170*
Rugova, Ibrahim, 2:211
Rumsfield, Donald H., 2:170, 2:359
Rusk, Dean, 1:325, 2:189, 2:198
Russia
aerial reconnaissance, 1:74
aircraft carrier development, 1:19–20
art and antiquities looting during 1917 Revolution, 1:46
Chechnya-Russian conflict, 1:172–173
intelligence and security, **3:30–31**
nuclear materials security issues, **3:31–33,** 3:38
Nunn-Lugar Threat Reduction Program, 3:32
Russian-Chechen referendum, 1:173
See also Soviet Union
Rutherford, Ernest, 2:294
Rwanda
genocide in, 1:7
terrorists in, 1:55
Rwandan Patriotic Front (RPF), 1:7

I S I

Sabotage, 3:*35,* **3:35–36**
Sadat, Pres. Anwar (Egypt), 1:59, 1:331
Safe Streets Act (1968), 2:195
Safire, William, 3:42
Sagan, Carl (scientist, 1934–1996), 2:376, 2:378
Salafist Group for Call and Combat (GSPC), **3:36**
Salmon, Daniel, 3:37
Salmonella and salmonella food poisoning, **3:37–38**
Sandia National Laboratory (SNL), 2:241, **3:38–39,** 3:*39*
vulnerability assessments, 3:245
Sanni, Violetta, 3:74–76
Santos-Dumont, Alberto (airship designer), 1:93
Sarin gas, 3:*40,* **3:40–41**
SARS. *See* Severe Acute Respiratory Syndrome (SARS)
Satellite imagery
monitoring accident sites, 1:187
remote sensing, 1:187, 2:425, 3:43–45
Satellites
commercial, 3:43–45
digital cameras in, 2:423
dual use technology, 1:364
Echelon, 1:370–372, 1:386
KH series surveillance cameras, 1:155–156
non-governmental, high resolution, 3:*43,* **3:43–45,** 3:*44*
nuclear device mishaps, 2:319–320
remote sensing, 1:187, 2:425, 3:43–45
space debris impact risk, 2:319
spy satellites, 1:187, 2:248
Satellite technology
altimetry measurements for bathymetric maps, 1:96
exports to the People's Republic of China, **3:41–42**
radar, 3:49
telemetry intelligence (TELINT), 3:48
Saudi Arabia, 3:*44*
Arab-Israeli wars, 2:273
intelligence and security, **3:50–51**
Savimbi, Jonas, 1:8

SBCCOM. *See* Soldier and Biological Chemical Command, U.S. Army (SBCCOM)
SBIRS. *See* Space-Based Infrared Satellite Systems (SBIRS)
Scanning and scanners
backscatter imaging, 3:53
coherent scattering, 3:53
computer tomography, 1:135, 3:52
EM wave scanners, 1:392–393
projection radiography, 3:51–52
retina and iris, 3:15–*16*
stereoscopic x-ray screening, 3:53
Scanning technologies, **3:51–53,** 3:*52*
Scanning tunneling microscopes, 2:271
Schabowski, Guenter, 1:106
Schaefer, Vincent Joseph, 2:259
Scherbius, Arthur (Enigma inventor), 1:205, 1:291, 1:405
Schlessinger, James R., 1:310
Schlieren system, 1:16
Schrader, Gerhard (chemist), 2:321–322
Schrödinger, Erwin, 2:295
Schroeder, Lynn, 2:452
Schulmeister, Charles, 2:297–298
Schwarzkopf, Gen. H. Norman, 2:414
Schweitzer-Pinochet letter forgery, 1:349
Science fiction media
Area 51, 1:51
movies, 2:288–289
Scotland Yard, 3:194
Scowcroft, Lt. Gen. Brent (security advisor), 2:30, 2:358
Clinton intelligence briefing, 2:429
Scramjet engines, 2:91–92
SEAL teams, **3:53–54,** 3:*54,* 3:*55*
Search and rescue programs, 2:341
Secret Intelligence Branch (SI, OSS), 2:390
Secret Service, U.S., **3:55–57,** 3:*56*
Secret writing, **3:58–59,** 3:*59*
steganography, 3:119–120
Secure Electronic Network for Travelers' Rapid Inspection (SENTRI), 2:439, **3:67–68**
Security, Infrastructure Protection and Counter-terrorism, U.S. National Coordinator, **3:62**
Security cameras, 1:156
closed circuit television systems, 1:219–220
perimeter security video and TV systems, 1:219–220
Security clearances
investigations, 1:322, **3:59–62**
levels of, 3:60
procedures for, 3:61–62
Security equipment
cameras, 1:156
closed circuit television systems, 1:156
DNA signatures, 1:342
motion sensors, 2:284–285
See also Security cameras
Security Oversight Board, 1:209
Security personnel, 2:4
Security Policy Board, U.S., **3:63**
Security systems
Closed circuit television systems (CCTV), 1:219–221
LoJack auto security and GPS, 2:*69*
procedures and equipment, 2:4–5
video motion detectors, 1:219
Seismology
forensic science, 2:35
monitoring explosions, **3:65**
Seismograph, **3:63–64**
Selassie, Haile (Ethiopian emperor), 1:7
Select Intelligence Committee (U.S. Senate). *See* Church Committee
Senate Intelligence Committee (U.S.), 1:32–33, 1:*202*
Senate Select Committee on Intelligence (U.S.), **3:66**
Senate Watergate committee, 3:*253,* 3:254
Sendero Luminoso (Shining Path, or SL), **3:66–67**
September 11 terrorist attacks, 1:26, 1:196, **3:68–72,** 3:*69,* 3:*70*
aftermath, 1:34–36
Bush, U.S. Pres. George W., 1:148, 3:70
CIA and, 1:201
emergency responses to, 3:70
FBI and, 3:71
international reactions to, 3:71
See also Pentagon; Terrorist attacks; World Trade Center
Sequencing, **3:72–73**
Serbia, intelligence and security, **3:73–74**
Sergeyev, Igor (Russian defense minister), 1:173
Severe Acute Respiratory Syndrome (SARS), 1:248–252
quarantine legislation for, 1:251
Sex-for-Secrets scandal, **3:74–76,** 3:*277*
Shamir, Adi, 1:286
Shayler, David, 2:*383*
Shepardson, Whitney H., 2:390
"Shoe bomber," **3:77**
Shoe transmitter, 3:*78,* **3:78**
Short-wave transmitters, **3:78–79**
Shuttle Radar Topography Mission, 2:248
Sicherheitsdienst (Nazi Security Service), 1:2
Sierra Leone, funding for civil war, 1:8
SIGINT (Signal Intelligence), **3:79–80**
sources, 1:193
use in Korean war, 2:209
Venona monitoring Soviet diplomatic communications, 3:228–231
Signal Intelligence Service (SIS, U.S. Army), 1:243–244, 2:390
Operation Magic, 2:386–387
Operation Shamrock, 2:388–389
Venona Project, 3:228–231, 3:*229*
Silencers (guns), **3:80–82,** 3:*81*
Sims, William, 3:103
Skunk Works (Lockheed Martin), **3:82–83,** 3:*83*
Sleep deprivation, countermeasures, 1:270
Slovakia, intelligence and security, **3:83–84**
Slovenia, intelligence and security, **3:84**
Smallpox, **3:84–85**
as a biological weapon, 1:124
science facilities for, 1:*169*
vaccination for, 2:*103,* 3:86
variola virus, 3:226–227
SMERSH (KGB assassination team)
Leon Trotsky, 1:61
poison pistols used by, 1:63–64
Smith, David L., 2:245
Smith, Don, 1:*308*
Smith, Gen. Walter Bedell, 1:195
Smith Act (1940), 2:7
Sniffer dogs, 1:164–165
Socialist Party (U.S.)
and Espionage Act (1917), 2:122
Socrates (c. 479–399 B.C.), 1:106
Sokolski, Henry, 3:42
Soldier and Biological Chemical Command, U.S. Army (SBCCOM), **3:88–89**
Solzhenitsyn, Aleksandr, 1:3
Somalia, 1:7
Al-Ittihad al-Islami (AIAI), 1:24
Operation Restore Hope, 1:*6*
Soman (nerve gas), **3:89–90**
Somoza Garcia, Anastazio, 1:28
Sonar, **3:90–91**
Sorenson, Paul S., 2:316
Sound surveillance system (SOSUS), **3:91–92**
South Africa intelligence and security, **3:92**
South African apartheid, 1:8
Southeast Asian Treaty Organization (SEATO), 1:237, 1:379
South Korea. *See* Korea, South
Soviet Union
Afghanistan invasion, 2:358
Antiballistic Missile (ABM) Treaty, 1:41–42
Berlin blockade, 1:99–101, 1:103
Cambridge University Spy Ring, 1:151–155, 3:96
Cuban Missile Crisis, 1:29, 1:293–295
disinformation in, 1:332–333, 2:203
Glasnost and anti-communism movements, 1:241
high power microwave weaponry, 2:272
intelligence and security, 1:75, 3:76–77, **3:93–96**, 3:230–231
Iran crisis, 1:231
jet aircraft in, 1:75
KGB, 1:102, 1:280–281, 1:331, 3:95–96
Marine mammal program, 2:249
Nixon's visit to China, 2:335

political parties and free elections in, 1:241
R-7 ICBM, 1:89
space stations, 3:97
Sputnik 1, 1:237
Strategic Arms Limitation Talks (SALT), 2:335
WW II U.S. relations with, 1:230–231
Space-Based Infrared Satellite Systems (SBIRS), 3:49
Spacecraft, 3:*83*
Institute of Future Space Transport concept, 2:*91*
Sputnik 1 (Soviet Union), 1:89, 1:237
Space debris
causes of, 2:320
cleanup options, 2:319, 2:321
collision avoidance, 2:320–321
in Earth orbit, 2:319–321
NORAD tracking, 2:345
Space environment
meteors as hazard in, 2:320
space debris impact risk, 2:319
Spaceflight early piloted flights, 1:89
Spacelab, 3:98
Spaceplanes, 3:99
Space shuttle
DOD payloads on, 2:299
military, 3:99
mission of, 2:299
orbiter, 3:97–98
propulsion systems, 3:98
Shuttle Radar Topography Mission, 2:248
Spacelab payloads, 3:98
Space shuttle Challenger, 2:299, 3:99–100
Space shuttle Columbia, 2:299
accident analysis, 1:259, 3:48, 3:100
GIS debris field mappng, 2:*65*
Space shuttle program, **3:96–100**
Space Stations, 3:97
Spain
aircraft carrier development, 1:19
First of October Anti-facist Resistance Group (GRAPO), 2:20
guerilla warfare by partisans, 2:74
intelligence and security, **3:101**
Spanish-American War, **3:101–103,** 3:*102*
Special Anti-narcotics Force (Bolivia), 1:133
Special Collection Service, U.S., **3:103–104**
Special Operations Command, U.S., **3:105**
Special Operations Executive, U.K. (SOE), **3:87–88**
Spectrometry
air plume analysis, 1:16–17
mass, 2:38
Spectroscopy, **3:107–109**
detection methods, 1:175, 1:184
nuclear activation analysis, 2:373
Spectrum, 1:382–383
Spertzel, Richard (U.N. weapons inspector), 1:334
Spores, 3:*109,* **3:109–111,** 3:244–245
SPOT satellite program, 1:187, 2:60
Sputnik 1 (Soviet Union), 1:89, 1:237, 2:298
Spy-in-the-sky intelligence, 1:237
satellite surveillance, 3:46
Soviet-Cuban missile emplacements, 1:196
spy planes, 1:197, 3:180–182
Spy novels, 2:130–132
Spy rings
Cambridge University Spy Ring, 1:151–155
Walker family spy ring, 3:249
Spy satellites, 1:197, 3:*45,* **3:45–50**
Air Force SAMOS and MIDAS satellites, 3:47
CORONA, 2:425, 3:46–47
DSP satellites, 2:427–248
film retrieval in reentry capsules, 3:46
KH "keyhole" series, 1:187, 1:310, 3:15, 3:46, 3:48
Soviet Union's, 3:47–48
types of intelligence from, 2:248, 3:48–49
SR-71 Blackbird, 1:76, 2:91, 2:425, **3:111–112**, 3:*112*, 3:116
Stalin, Joseph (1879–1953), 1:230, 1:231, 2:207
Cold War declaration, 1:233
death of, 1:235
Star Wars (SDI). *See* Strategic Defense Initiative (SDI)
STASI (East German intelligence agency), **3:114–115,** 3:*115*
State Department, U.S., 1:55, **1:324–326**
bureaus and offices, 1:326
Coordinator for Counter-Terrorism, 1:270–271
intelligence agencies in, 3:204
Secretaries of State, 1:325
Stealth technology, **3:115–119,** 3:*316*
B-2 Bomber, 1:79
F-117A Stealth Fighter, 2:*2*
Steganography, **3:119–120**
Stereoscopic scanning
x-ray screening, 3:53
Sterilization, 2:244
Stevenson, Adlai, 1:98
Stieber, Wilbur, 1:2
Stockpile Stewardship and Management Program (SSMP), 2:225
Straight, Michael, 1:154
Strassman, Fritz, 2:22, 2:375
Strategic Air Command, U.S. (SAC), 2:237
Strategic Arms Limitation Talks (SALT), 1:76, 1:238, 2:335
Strategic Arms Limitation Treaty (SALT II), 1:166–167
Strategic Arms Reduction Treaty (START), 1:76, 1:240, 2:377, 3:9, **3:112–313**
Strategic Arms Reduction Treaty (START II), **3:113–314**
Strategic Command, U.S., **3:220**
Strategic Defense Initiative (SDI), 1:*121,* 1:240, 3:9, **3:120–125**
Stun guns
Taser, 3:134–*135*
Sturgeon (U.S. submarine), 3:188–189
Submarines
espionage and the use of, **3:188–190,** 3:*189*
sonar for underwater navigation, 3:90
Soviet, 3:189–190
United States, 3:188–189
Substance Abuse and Mental Health Services Administration (SAMHSA), 2:455
Sudan, U.S. attacks on, 2:274
Sudan intelligence and security, **3:126**
Suez Canal, 1:404–405, **3:127**
Sung Li, 1:373
Supercomputers, **3:128,** 3:*129*
Surveillance cameras, 1:155–156
copy and robot cameras, 1:156–157
in Eastern Europe, 1:156
See also Reconnaissance aircraft; Reconnaissance satellites
Surveillance systems
closed circuit TV systems, 1:220–221
Echelon, 1:370–372, 1:386
Sutcliffe, R.C., 2:256
Sverdlovsk, Russia, 1:*235*
Sweden, intelligence and security, **3:130**
Switzerland, intelligence and security, **3:131**
Symington, W. Stuart, 1:13
Synge, Richard, 2:49
Synthetic aperture radar (SAR), 2:59, 2:60, **3:2–3,** 3:14
Syria, intelligence and security, **3:131–132**
SZ42 Cipher, 1:205
Szilard, Leo, 1:231, 2:246

T

Tabun (nerve gas), **3:133**
Taft-Hartley Act (1947), 2:122
Taiwan
intelligence and security, **3:134**
Tachen Straits crisis, 1:237
Taliban and Al-Qaeda (Afghanistan), 1:27, 2:125, 2:274, 3:68
Tanaka memorandum forgery, 1:346–347
Tariff Act (1789), 1:296
Taser, **3:134–135**, *3:135*
Taxpayers, protection of rights, 2:137
TCG (Tunisian Combatant Group), **3:175**
Technical intelligence (TECHINT), **3:136**
Technology

preventing counterfeit currency, 1:274
Technology Applications Program (BMDO), 1:86
Technology sharing between U.S. and U.K., **3:106–107**
Technology Transfer Center, National (NTTC), **3:136–137**
Telecommunications policy
National Security Telecommunications Advisory Committee, 2:311
National Telecommunications Information Administration, U.S. (NTIA), 2:312
Telecommunications Act (1996), 2:10
Telegraph
cryptography and the, 1:419
foreign transmissions monitored, 2:388–389
Telemetry, **3:137**
Telephone Caller Identification (Caller ID), **3:137–138**
Telephone recording laws, **3:138**
Telephone recording system, **3:139**
Telephone scrambler, **3:139**
Telephone tap detector, **3:140**
Teller, Edward, 2:375
TEMPEST technology
as electronic intelligence, 1:385
Tenebaum, Ehud, 1:*256*
Tenet, George J., 1:*194,* 1:196, 1:311, 1:*328,* 2:168
Terrain intelligence, **2:58–59**
Terror alert system, U.S., **3:140–142,** 3:*141*
Terrorism, domestic (U.S.), **3:142–146**
Terrorism, history and ideology
anarchism as ideological force, 3:148
philosophical origins, **3:148–150,** 3:*149*
Terrorism, intelligence based on
Australian intelligence, 1:72
computer and internet technologies aiding, 2:8–9
drug traffic and narco-terrorism, 1:281, 1:314
financial intelligence, 3:157–158
GAO threat and risk assessment report, **3:146–147,** 3:*147*
Terrorism Act (U.K.), **1:142**
Terrorist attacks
bombings, 1:48
CIA and, 1:201
domestic, 2:126
drug traffic and narco-terrorism funding, 1:281, 1:314
terrorism risk insurance, 3:151
See also September 11 terrorist attacks; World Trade Center
Terrorist Information Awareness (TIA) system, 1:22, **3:162**
Terrorist organizations
use of asymmetric warfare, 1:68
financing of, 3:157–158
freezing of assets, **3:155–160**
international, 1:1
nuclear materials trafficking reported, 3:32
para-state organizations, **3:151–154,** 3:*152,* 3:*153*
state-sponsored, 3:154
Terrorist organization list, U.S., **3:154–155**
Terrorist Threat Integration Center, 1:149, **3:160–161**
Teten, Howard, 2:449
Tethered Aerostat Radar System (U.S. Air Force), 1:94
THAAD. *See* Theater High Altitude Area Defense (THAAD)
Thailand, 1:19
Theater High Altitude Area Defense (THAAD), 1:86
Think tanks, 2:342
Thin layer chromatography, 2:38, **3:161–162**
Thithmius (16th century German monk), 1:289
Thomson, Sir J.J., 2:49, 2:294
Three Mile Island nuclear accident, 2:24, 2:372
Threshold Test Ban Treaty, 1:253–254
Thyroid gland cancer therapy, 2:443
TIA. *See* Terrorist Information Awareness (TIA); Total Information Awareness (TIA)
Tiselius, Arne, 1:391
Tissue-based biosensors, **3:163**
Tissue engineering, 1:111–112
Toguri, Iva Ikoku, 3:163–*164*
Tokyo Rose, 2:450, **3:163–164**
Tolbert, Pres. William (Liberia), 1:8
Tolman, Dr. Richard, 2:*246*
Tomahawk cruise missile, 1:284–*285*
Tomography
computer, 1:22, 1:135–136, 3:52
Topography and topographic maps, 2:248
military use of terrain intelligence and, 2:58–59
radar mapping, 2:59
Shuttle Radar Topography Mission, 2:248
Torpedoes, in Civil War, 1:211
Torture techniques and technologies, **2:152–155,** 2:*153*
Total Information Awareness (TIA), 1:22, 2:146
Tournament of Shadows, 2:71–72
Townsend, Robert, 3:22
Toxicology, **3:164–165**
Toxic spills reporting
Coast Guard National Response Center, 1:223
Toxic Substances and Disease Registry, Agency for (ATSDR), 2:455
Toxins, **3:166–167**
Anthrax, 1:33–34
APS analysis of toxin structure, 1:53
mapping concentration and distribution of, 1:113
vaccines for, 3:167
Trade craft, **3:167**
Trading with the Enemy Act (1941), 3:171
Traffic surveillance system, 1:*357*
Transportation Department, U.S., 3:*168,* **3:168–169**
intelligence agencies in, 3:204
Transportation Security Administration (TSA)
airport screeners, 1:77–78
aviation security in U.S., 1:209, 3:72
Federal Air Marshalls, 1:14
Treasury Department, U.S., **3:169–171,** 3:*170*
freezing of terrorist assets, 3:155–156
international monetary policy (post WW II), 3:171
Operation Green Quest, 3:158
Treaty of Versailles, 2:226
Tritium, 2:81–82
Trotsky, Leon, 1:61
Trudeau, Pierre Elliot (Canadian Prime Minister), 1:162
Truman administration (1945–1953), 1:200
atomic bomb use on Japan, 1:231
Cold War policy and Truman Doctrine, 1:231–232, 1:233, 3:172
hydrogen bomb request, 1:232
national security policy, **3:171–172**
Truth serum, **3:173–174**
TSA. *See* Transportation Security Administration (TSA)
Tularemia (disease), **3:174–175**
Tunisian Combatant Group (TCG), **3:175**
Tunisian Islamic Fighting Group, 3:175
Tunner, Maj. Gen. William H., 1:100
Tupac Amaru Revolutionary Movement (MRTA), **3:175**
Turing, Alan
cryptography and Enigma, 1:407, 3:184
Turing bombe development, 1:137, 1:206, 1:242
Turkey, intelligence and security, **3:176**
Turkish Hizballah, **3:176**
Turner, Admiral Stansfield, 1:310
TV shows
espionage and intelligence portrayals, 2:288–289
Get Smart, 3:78
Typex cipher machine, **3:177**

U

U-2 spy plane (U.S.), 1:*74,* 1:237, **3:180–182,** 3:*181*
design of, 3:182

Russian capture of, 1:76
U-2 incident, **3:179–180**
UAV. *See* Unmanned Aerial Vehicles (UAV)
See also U-2 spy plane (U.S.)
Ukraine, intelligence and security, **3:183**
UKUSA. *See* United Kingdom—United States of America Security Agreement (UKUSA)
Ullman, Harlan K et. al.
Shock and Awe: Achieving Rapid Dominance, 2:107
Ulster Defense Association (UDA), **3:183**
Ulster Freedom Fighters (UDA/UVF), **3:183**
Ultra, Operation, **3:184–185**
Ultra-high pressure sterilization, 2:244
Ultraviolet spectroscopy, 3:107–108
Ultraviolet waves, 1:383
Un-American Activities Committee, U.S. House (HUAC), 2:122–123, 2:252
Underground facilities, U.S. Government, **3:186–188,** 3:*187*
UNESCO. *See* United Nations Educational, Scientific and Cultural Organization (UNESCO)
Unexploded ordnance and mines. *See* Land mines clearance programs; Munitions, unexploded ordnance clearance programs
Unidentified flying objects (UFO's)
Area 51, 1:51
government study of, 1:75
Union balloon corps (Civil War, U.S.), 1:92
UNITA. *See* National Union for the Total Independence of Angola (UNITA)
United Airlines, hijacked flights—9/11, 3:69
United Kingdom
aircraft carrier development, 1:19
assassination attempts on N. Bonaparte, 2:297
Berlin Airlift operations, 1:100
counter-terrorism policy, **3:193**
D Notice system, 1:305
espionage in 19th century France, 2:296–298
intelligence and security, **3:194–195**
intelligence on Iraqi weapons programs, 2:167–168
United Kingdom—United States of America Security Agreement (UKUSA), 3:106–107
United Nations
blocking terrorist financing, 3:158–159
Security Council, **3:196–198,** 3:*197*
war crimes tribunal, 2:211
United Nations Educational, Scientific and Cultural Organization (UNESCO)
protection of artifacts convention, 1:47
United Nations Security Council
China and, 1:189
Iraq and Resolution 1441, 2:164
Resolution 1373, 1:160–161
United Self-Defense Forces/Group of Colombia (AUC), **3:198**
United States
America enters World War II, 3:279–280
bombing of embassy and barracks in Lebanon, 2:227–*228*
counter-terrorism policy, **3:198–201,** 3:*199*
Cuban Missile Crisis, 1:29
hostages in Iran, 1:166
OPEC and Middle East oil dependency, 1:166, 1:238
U.S. Army
Operation Sea Spray, 1:118
School of the Americas, 1:29
U.S. Atomic Energy Detection System (USAEDS), 1:12–13
U.S. Congress
classified information leaked from, 1:*214*
oversight of Intelligence community, 2:130, 2:135–136
United States elections
Civil Rights Commission study on Florida balloting of Nov. 2000, 1:247–248
United States foreign policy
containment of Soviet expansionism, 2:189, 2:206–207
Monroe Doctrine and, 2:281–282
State Department and, 1:325
United States intelligence and security, 3:202–205
Chinese espionage in, 1:190–191
CIA foreign intelligence, 1:193
dawn of professional, 3:207–208
domestic, 1:192
Foreign Intelligence Advisory Board, 1:194
history of, **3:206–209**
intelligence history and historical records, 1:197
intelligence sources, 1:193
Senate Select Committee on Intelligence, 1:192, 1:194
See also CIA
United States military
bombing of U.S. marine barracks in Lebanon, 2:227–*228*
Reagan's buildup of, 1:240
United States security policy and interventions
Africa, 1:5–9
Latin America, 1:28–31
United States—Soviet relations
capitalism *vs.* socialism, 1:232, 1:233
Cold War, 1:230–232
Nixon's arms reduction talks, 1:238
in Poland, 1:233
United States Special Forces
in Afghanistan, 1:60
Delta Force, 1:322–323
United States technology
Chinese interest in, 1:191
dual use technology, 1:364–365
Eisenhower's innovation policy, 1:235
source literature on, 1:191
Unmanned Aerial Vehicles (UAV), **3:209–210,** 3:*210*
as reconnaissance aircraft, 1:*27,* 1:51, 1:76
Uranium, **3:211–212,** 3:*212*
converted to commercial use, 1:355
depletion weapons, 1:333–334, **3:212–213**
nuclear fission using, 2:22–23
Uranium, weapons grade, 1:231
enrichment processing facility, 1:*235*
tracking nuclear materials, **3:255–257**
Urbani, Dr. Carl (SARS identification), 1:249
USAEDS. *See* U.S. Atomic Energy Detection System (USAEDS)
USAMRIDC (Medical Research Institute of Chemical Defense, U.S. Army), **3:213–214**
USAMRIID (Medical Research Institute of Infectious Diseases, U.S. Army), 3:*214,* **3:214–216**
USCSB. *See* Chemical Safety and Hazard Investigation Board (USCSB, U.S.)
USS *Cole,* **3:216–217**
USS *Liberty,* **3:218–220,** 3:*219*
USS *Maine* sunk near Cuba (1888), 3:101–102, 3:*102*
USSTRATCOM. *See* Strategic Command, U.S.

V

V-2 ballistic missile, 1:87, 1:89
Vaccination, **3:221–222**
Vaccine development
at Brookhaven National Laboratory, 1:143
at FDA, 2:10–11
production and, 3:224–225
Vaccines, **3:223–226**
anthrax, 1:37–39, 1:39, 3:221
genetic engineering of, 3:86
livestock, 2:427
rabies, 3:223
Salk polio, 1:168, 1:170, 3:224
smallpox, 2:*103,* 3:85, 3:86, 3:223
storage, 2:427
toxins, 3:167
Vanunu, Moredechai, 2:*182*
Variola virus (smallpox), 3:84, **3:226–227**
Venezuela, intelligence and security, **3:227–228**
Venona, **3:228–231,** 3:*229*
Vernam, Gilbert, 1:207, 1:242, 1:291

Vibrational spectroscopy, 3:108–109
VICAP. *See* Violent Criminal Apprehension Program (VICAP)
Victims of Crime Act (1984), 2:195
Viet Minh (League for the Independence of Vietnam), 3:231
Vietnam
  Army Security Agency (ASA, U.S.), 1:56
  escalation of U.S. involvement in, 2:189
  first to control SARS outbreak, 1:251
  Geneva Accords division of, 3:232
Vietnam, South
  Phoenix Program operations in, 2:420–421
  U.S. support of, 2:188
Vietnam War, **3:231–236,** 3:*232,* 3:*233*
  Agent Orange, 1:9–10
  Agent Orange used in, 1:9–10
  beginnings of, 1:237
  CIA involvement in, 3:234–235
  napalm attacks by U.S., 1:*181*
  Nixon's pull-out from, 2:334, 3:234
  Tet Offensive, 3:233–234
  Tonkin Gulf Resolution, 2:189, 3:233
  U.S. loss of S. Vietnam to communists, 2:30, 3:234
Vigenere, Blaise de, 1:289
Villa, Pancho, 1:28
Violent Criminal Apprehension Program (VICAP), 2:449–450
Viral biology, **3:236–240,** 3:*237*
Viral exposure therapy, antiviral drug development, **3:241**
Virology, 3:236–238
  anti-viral drug development, 3:241
Virtual reality modeling language (VRML), 1:259
Viruses
  identification of, 3:238
  replication, 3:239–240
Visible light waves, 1:382–383
Voice alteration, electronic, **3:242**
Voice analysis, 2:39–40
Voice of America (VDA), U.S., 3:*243,* **3:243–244**
Vonnegut, Bernard, 2:259
Vozorzhdeniye Island (Russia) biochemical weapons test facility, **3:244–245**
Vulnerability assessments, **3:245**
VX agent, **3:246–247**

W

Walker, Jr., John A., 1:159, 1:275, 1:361, 3:249
Walker, Michael Lance, 3:249
Walker, William, 1:28
Walker family spy ring, 2:280, **3:249**
Wallis, John, 1:128
Ward, Henry, 3:103
Warner Brothers spy movies, 2:287
War of 1812, **3:250–251**
War Powers Act of 1973 (Bolland Amendment), 1:30
Warren, David, 2:25
Wartime plunder, 1:45–48
Washington Naval Limitation Treaty (1922), 1:19
Watergate break-in, 1:202, 2:28, **3:253–254**
Water supply
  contamination/decontamination, 1:10–11, **3:251–252**
  counter-terrorism threat to, 3:251–253
  EPA monitoring, 1:127
Weapon inspections
  Iran, 2:161
  Iraq, 2:*163*–166
Weapons
  bludgeons and blunt instruments, 1:64
  Confederate infernal, 1:211
  energy directed, 1:399
  knives and edge weapons, 1:64
Weapons of mass destruction (WMD), **3:257–259**
  detection, **3:260–263**
  Iraq, 2:167–168, 2:169–176
Weather alteration, 2:259–260
  cloud seeding, 2:257, 2:259–260
Weather forecasting
  National Weather Service, 2:257
  types of forecasting, 2:258–259
  weather and Doppler radar, 2:256–257, 2:*257*
Weathersby, Katherine, 1:332
Webster, Daniel W.
  Comprehensive Ballistic Fingerprinting of New Guns, 1:*85*
Webster, William H., 1:196, 1:311, 2:8
Weinberger, Casper W., 2:156–157, 2:358
Weinberger SDI speech forgery, 1:348–349
Weitling, Wilhelm (1808–1871), 3:150
Welch, Joseph, 2:253
Wen Ho Lee, 1:190, 1:191, 1:*213,* 2:133
Westmoreland, Gen. William C., 3:233
West Nile virus, 2:104
Whalen documents forgery, 1:347
Wheatstone, Sir Charles, 2:426
Whistleblower protections
  cases, 3:105
  Office of Special Counsel (OSC), **3:104–105**
  Whistleblower Protection Act (1989), 3:104
Whitworth, Jerry Alfred, 3:249
WHO. *See* World Health Organization (WHO)
Wickham, William, 2:296
Wilson, Vice Admiral Thomas R., 1:*303,* 1:*328*
Wilson, Woodrow
  League of Nations and Nobel Peace Prize, 2:226
Windtalkers (Navaho Indians), 1:291, **3:263–265,** 3:*264*
Wise, John (military use of balloons), 1:92
Witt, James L. (FEMA director), 2:16
Women
  cryptography opportunities (WW II), 1:131, 1:137
  spies in the Civil War (U.S.), 1:211
  Women Accepted for Voluntary Service Corps (WAVES), 1:137
Woodward, Bob, 1:202
Woodward, Gilbert, 2:458
Woolsey, R. James, 1:196, 1:311
World Bank, 2:99
World Health Organization (WHO), 1:249, 3:85, **3:265–266**
World Islamic Front for Jihad
  Al-Qaeda and the Egyptian Islamic Jihad, 1:26
World Trade Center, 3:*14,* 3:*69*
  history and construction, 3:268–269
  9/11 aftermath and heroism, 3:269–270
  9/11 attack, 1:26, 1:34–36, 1:196, 3:268–270
  1993 bombing, 1:23, 1:134, 1:276, **3:266–268,** 3:*267*
  tower collapse study, 1:50, 1:*245*
  See also September 11 terrorist attacks
World War I, **3:270–274**
  Black Tom explosion, 1:128–130
  chemical warfare in, 1:180–181
  costs of, 3:170
  federal investigators in, 2:6
  French protection of the Louvre's collection, 1:46
  German code books captured by British, **3:274–275**
  German cryptography, 1:3–4
  German intelligence agency, 1:2
  Treaty of Versailles, 2:226
World War II, **3:275–282**
  Allies victories, 3:280–281
  Axis victories, 3:278–279
  CIA monitored broadcasts, 1:199
  Combined Chiefs of Staff (U.S.—Britain), 2:190
  Commissar Order (Germany), 1:3
  FBI involvement in, 2:7
  French protection of the Louvre's collection, 1:47
  French resistance shuttling Allied servicemen, 2:43
  Italian Army surrender, **3:283–284**
  Operation Mincemeat and Sicily invasion, **3:282–283**
  Pearl Harbor attack, 2:410–413
  Radio Tokyo and Tokyo Rose, 3:163–164
  reconnaissance aircraft, 1:75

How to go to your page

U.K.-U.S. agreements to share information, 3:106–107
World Wide Web, 1:171–172
World Wide Web browsers, 2:142
Wrath of God, 1:61–62, 2:283–284
Wright, Orville, 2:298
Wright, Peter, 1:404
Wyler, Valeriano (Cuban leader), 3:101

X

X-15 aircraft, 2:90–91
X-ray fluorescence, 3:108
X-ray machines
backscatter imaging, 3:53
CT scanners, 3:*52*
as detection devices, 1:135
used in passenger screening process, 1:22
projection radiography scanning, 3:51–52
stereoscopic x-ray screening, 3:53
technology refined, 1:175
X-ray photoelectron spectroscopy, 3:108
X-rays, medical and security uses, 1:383

Y

Yale, Jr., Linus, 2:236
Yamasaki, Minoru, 3:268
Yardley, Herbert Osborne ologist), 1:128
Yeager, Charles E. "Chuck," 2:90
Yelsimov, Alexi, 3:75
Yeltsin, Pres. Boris (Russian), 1:*148,* 1:172–173, 1:241
Yersin, Alexandre, 1:144
Yersinia pestis. See Bubonic plague
Yom Kippur war, 2:284
Yoshikawa, Takeo, 2:412
Young Hegelians, 3:148
Yousef, Ramzi, 1:276
Yucca Mountain, Nevada, 3:6–7
Yugoslavia, Federal Republic, 1:138
Croatia and, 1:284

Z

Zaire. *See* Congo
Zapp, Walter, 1:158–159, 2:267
Zeppelin, Ferdinand von, 1:93
Zimmermann, Arthur, 1:290
Zimmermann, Philip R., 1:291, 2:446
Zinn, Herbert, 1:256
Zinoview, Grigory, 1:346
Zinoview letter forgery, 1:346
Zoonoses, **3:286–287**